Security Escort

SE2000 Series

BOSCH

en Training Manual

Table of contents

1	**System overview**	**7**
1.1	What is Security Escort?	7
1.2	Emphasis on reliability	7
1.3	System applications	7
1.4	Some example installations	7
1.5	Other system applications	8
1.6	Security Escort features	8
1.7	System components description	9
1.8	Compatible parts	10
2	**System components/specifications**	**11**
2.1	Central Console	11
2.2	SE3 subscriber transmitter	12
2.3	SE2 personnel transmitter	14
2.4	SE3401 asset tracking transmitter	15
2.5	RF3401 asset tracking transmitter	16
2.6	SE88 panic transmitter	17
2.7	SEFD1 transmitter	18
2.8	EA102 receiver	19
2.9	EA500 transponder	20
2.10	EA120 alert unit	21
3	**Equipment estimation, location accuracy and receiver location**	**23**
3.1	Location accuracy	23
3.2	Pre-bid equipment estimation	24
3.2.1	Initial equipment estimate	24
3.3	Pre-construction coverage verification survey	26
3.3.1	Verify each potential receiver location	26
3.3.2	Indoor receiver installation	28
3.3.3	Outdoor receiver installation	28
4	**System wiring**	**30**
4.1	General guidelines	30
4.1.1	Transponder - SE485 wiring table	30
4.1.2	Observe established standards	31
4.2	Component wiring guidelines	31
4.2.1	General wiring diagram	31
4.2.2	Transponder information sheet	33
4.3	EA500 transponder	36
4.3.1	General	36
4.3.2	Specifications	36
4.3.3	Mounting	36
4.3.4	Wiring	36
4.3.5	Set the address	37
4.4	EA102A-304 receiver	39
4.4.1	Specifications	39
4.4.2	Mounting	39
4.4.3	Wiring	40
4.4.4	Switches and jumpers	41
4.4.5	Pre-wired installations	43

4.4.6	Drilling templates	43
4.5	EA120B alert unit	45
4.5.1	Specifications	45
4.5.2	General information	46
4.5.3	Mounting	46
4.5.4	Wiring	47
4.5.5	Set the address	47
4.6	Moxa interface	47
4.6.1	Introduction	47
4.6.2	Specifications	48
4.6.3	Installation and operation notes	48
4.7	Lantronix interface	50
4.7.1	Introduction	50
4.7.2	Specifications	50
4.7.3	Installation and operation notes	50
4.8	SE485 interface	54
4.8.1	Introduction	54
4.8.2	Specifications	54
4.8.3	Installation and operation notes	54
4.9	ProxLink setup	55
5	**Installation options**	**59**
5.1	Demo installations	59
5.2	Non-Network installations	59
5.3	Network installations	59
5.4	Installing the Security Escort software	60
5.4.1	Software installation procedure	60
5.4.2	Image files	68
6	**Central Console, computer setup and programming**	**70**
6.1	Transponder comm port setup	70
6.2	Remote comm port setup dialog	70
6.3	Remote setup dialog	72
6.4	Transponder Database	75
6.4.1	Transponder information sheet	76
6.4.2	Transponder Database dialog	79
6.4.3	Creating a new transponder entry	82
6.4.4	Modifying existing transponder entry	83
6.4.5	Setting receiver parameters	83
6.4.6	Alarm area setup	90
6.5	Powering up the system for the first time	91
7	**Troubleshooting transponders, points, receivers, and alert units**	**95**
7.1	Common errors	95
7.2	Built-in troubleshooting aids	95
7.2.1	Receiver	95
7.2.2	Transponder	97
7.3	Troubleshooting reference	100
7.3.1	Transponder communication with SE485 bus	100
7.3.2	Transponder communication with ProxLink	101
7.3.3	Transponder communication with Moxa/Lantronix device	103
7.3.4	EA500 transponder bus faults	104

7.3.5	EA102 receiver issues	105
7.4	Receiver configuration dialog	108
7.5	Post construction setup	110
7.5.1	Testing the location accuracy of an installation	110
7.5.2	Improving the location accuracy of an installation	112
7.6	System preferences dialog	113
7.7	Security Preferences dialog	118
7.8	System Defaults dialog	123
7.9	System Labels dialog	124
7.10	Subscriber Database	125
7.10.1	Print Subscriber Database	126
7.10.2	Edit Subscriber Database record	127
7.10.3	Additional subscriber information	131
7.10.4	Subscriber images	132
7.10.5	Fixed Location Transmitters	133
7.10.6	Subscriber (individual) Pager Setup	134
7.10.7	Subscriber Database Advanced Features	135
7.11	Schedules dialog	140
7.11.1	Ignore Holidays for this schedule	141
7.11.2	Edit Schedule Times dialog	142
7.11.3	View Alarm Groups dialog	143
7.11.4	Alarm Groups dialog	144
7.11.5	Alarm Group State dialog	145
7.11.6	Current Check-in Status dialog	145
7.12	Exporting, importing and merging the Subscriber Database	146
7.12.1	File format of "TABMERGE.DAT" / "TABMERGE_EXPORT.DAT"	147
7.12.2	Exporting the Subscriber Database	153
7.12.3	Importing the Subscriber Database	153
7.12.4	Merging the Subscriber Database	155
7.13	Exporting and importing the Transponder Database	155
7.13.1	File format of "TRANSMERGE.DAT" / "TRANSMERGE_EXPORT.DAT"	156
7.13.2	Exporting the Transponder Database	164
7.13.3	Importing the Transponder Database	164
7.14	Operator Database	166
7.14.1	Edit Operator Database record	166
7.14.2	Authority levels	167
7.15	Reports Database	168
7.15.1	Report statistics	169
7.15.2	Map	170
7.15.3	Edit data	170
7.15.4	Delete	171
7.15.5	Locate Key	171
7.15.6	Key Select	172
7.15.7	Incomplete	172
7.16	System redundancy	172
7.16.1	Automatic redundancy	173
7.16.2	Manual redundancy	173
8	**System menus and dialogs**	**174**
8.1	File menu	174

8.1.1	Locate transmitters	174
8.1.2	Maintenance alarm database	174
8.1.3	Transmitter Change	175
8.2	Utilities menu	178
8.2.1	Backup dialog	178
8.2.2	Restore dialog	180
8.2.3	Print/Export System Reports	182
8.2.4	Export Alarm Reports	184
8.2.5	Clear Screen	185
8.2.6	Output verification	185
8.2.7	Synchronize System Time	185
8.3	Setup commands	185
8.3.1	Show History	186
8.3.2	History Filter Dialog	186
8.3.3	Popup Trouble Filter	189
8.3.4	Transponder Parameter Change	194
8.3.5	Transponder Data View	195
8.3.6	Receiver configuration dialog	197
8.3.7	Receiver test dialog	200
8.3.8	Network status dialog	202
8.3.9	System status dialog	204
8.3.10	Pager setup dialog	205
8.3.11	Send pager message dialog	207
8.4	Print history screen	208
8.4.1	Print file dialog	208
8.5	Network menu	209
8.5.1	System Directories and Network Address Dialog	210
8.5.2	Network Socket Status Dialog	213
8.5.3	Computer's Winsock Data Dialog	215
8.5.4	Computer's Name and Address Dialog	215
8.6	About menu	215
8.6.1	About dialog	217
9	**Files required for Security Escort**	**220**
10	**Appendix: Software licenses**	**225**
10.1	Bosch software	225
10.2	Other licenses — copyright notices	225
10.3	Warranties and disclaimer of warranties	225
	Index	**226**

1 System overview

1.1 What is Security Escort?

- Unique multiple user help call and asset tracking system
- Identifies user information and location, by floor, above or below ground
- Small, easy to carry transmitters
- Indoor/outdoor protection for 60,000+ users and assets as well as multiple buildings
- Man-down alarm, officer tracking & guard tour
- Post-alarm tracking and alarm map recall
- System capabilities perfect for campus and community environments

1.2 Emphasis on reliability

- Supported by a multi million dollar company
- Extensive field testing under maximum abuse conditions, from -20°F to +120°F
- Supervised system communication
- Low battery user *and* system operator notification
- Archived retrieval of system activity
- Patented technology
- Post alarm transmitter tracking
- System-wide backup power feature

1.3 System applications

- Student Safety
- Officer Tracking
- Guard Tour
- Employee/Faculty Security
- VIP Protection
- Executive Protection
- Man-Down
- Asset Tracking

1.4 Some example installations

Educational Facilities:
- Florida Southern, FL
- Oswego State, NY
- Nazareth College, NY

Healthcare Facilities:
- New Hanover Medical Center, NC
- Provo Psychiatric Hospital, Utah
- Fairport Retirement Home, NY

Correctional Facilities:
- Westchester County D.O.C., Valhalla, NY
- Immigration & Naturalization Facility, TX
- US Naval Brig, SC

Other:
- Diamond Mines, South Africa
- Amusement Park, FL
- International Art Museum, NY

1.5 Other system applications

- Hotels & Casinos
- Amusement Parks
- Commercial Complexes
  - Buildings
  - Parking Lots/Garages
- Museums
- Financial Institutions
- Child Care Facilities

1.6 Security Escort features

The Security Escort System is engineered to provide reliability and user ease of operation. Our patented feature set allows for customization and integration in any installation. These features ensure system integrity and the comfort that when assistance is needed, help is just a click away.

User Self Test

- Assures you that your transmitter is working
- Battery condition sent with every transmission
- Each test verifies system integrity
- Logs each test performed for easy access and reporting
- Can be performed indoors and outdoors
- Ensures user acceptance and peace of mind

Asset Tracking

- Location of assets
- Protection against removal
- Wireless sensing
- No re-cabling for asset relocation
- Auto tracking and location identification

Fixed Point Identification

- Allows for identification of any fixed point
- Simple system integration
- Expands over all system capability and functionality

1.7 System components description

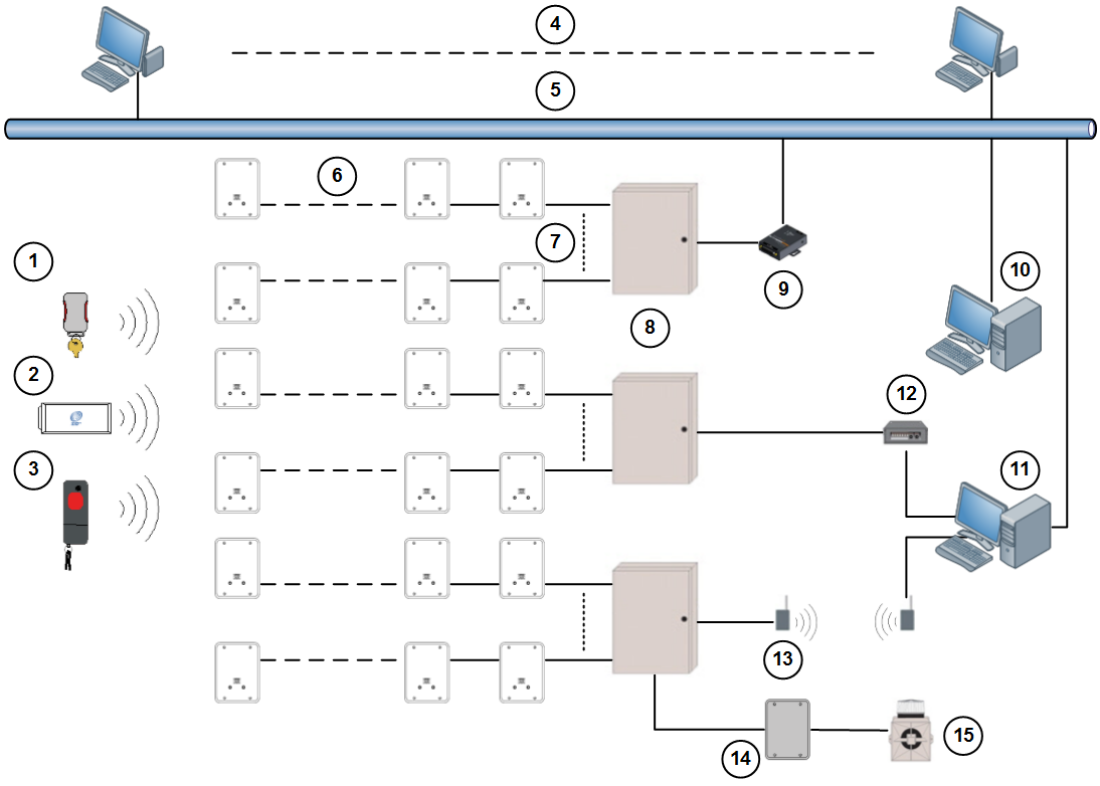


Figure 1.1: System Block Diagram

1	Subscriber transmitter	9	Serial to Ethernet interface
2	Point tracking transmitter	10	Slave workstation
3	Personnel transmitter	11	Master workstation
4	Up to 8 workstation	12	SE485 interface
5	LAN	13	Spread spectrum wireless links
6	Up to 8 receivers	14	Alert unit
7	Up to 8 bus	15	Strobe
8	Transponder		

The **transmitter** is a miniature, hand-held radio transmitter used to transmit either a distress or a test signal. The **receivers** are located throughout the protected area and detect the radio transmissions from transmitters. Alert units are siren/strobe units activated in the event of an alarm. Transponders are devices that control groups of receivers and alert units, connected to them by wire. Each transponder relays alarm and test signals from its receivers to the Central Console. In addition, the transponder tests for device and wiring faults, and transmits problem conditions to the Central Console. The **Central Console** consists of a computer (plus an optional backup and up to 8 optional workstations) which receives alarm and trouble signals from the transponders, analyzes the signals, activates strobes and sirens on the alert units, and produces a display for the Security dispatcher. Each of these system elements is described more fully in the sections that follow.

1.8 Compatible parts

The following table indicates the parts available for inclusion in a Security Escort system. Contact Bosch Security Systems Customer Service for up-to-date model numbers.

Part Name	Description
Electronics, Components	
EA500	Electronics for eight-bus transponder
EA102	Electronics for indoor or outdoor receiver
EA120	Electronics for indoor and outdoor alert unit
SE485	Interface between transponder and Central Console
SE2 transmitters	Man-down, lanyard, supervisory, and duress transmitter
SE3401	Point tracking transmitter
SE88	Personal watch/Pendant transmitter
Enclosures and Housings	
AE3	Large enclosure, 51.5 cm x 37.5 cm (20.25 in x 14.75 in)
AE1	Small enclosure, 36.8 cm x 31.8 cm (14.5 in x 12.5 in]
AE100	Indoor receiver enclosure
AE101	Outdoor receiver enclosure
Software	
SE2005	System software for up to 500 users
SE2010	System software for up to 1,000 users
SE2050	System software for up to 5,000 users

2 System components/specifications

2.1 Central Console

Description

The Central Console consists of one or two computers (and up to 8 additional workstations) running the Security Escort software within the Microsoft Windows environment. One computer serves as the master controller for the entire Security Escort system and the second slave computer serves as a back-up. The slave computer can be used for administrative functions such as adding subscribers or performing routine system tests without interfering with the operation of the main computer. The workstations can perform all normal Security Escort functions with the exception of communicating with the transponders.

Software overview

The Central Console contains all of the operating software and all of the databases required by the Security Escort system. The installation and maintenance portion of the Security Escort software is designed to facilitate set-up and modification of the system and to provide rapid diagnosis of system problems, usually with only one person being required. The system software also continually monitors the status of each transponder to ensure it is functioning correctly.

Versions

There are several versions of the software available. The number of users the system will support defines each version. The following table lists the available models and the number of supported users:

Model	User Base
SE2005	500
SE2010	1,000
SE2050	5,000

Notice!

For systems supporting more than 5,000 users contact Bosch Security Systems Sales.

Minimum system requirements

As a minimum, each computer in the Central Console should be equipped with the following features and components:

- **Processor:** 1 GHz or faster.
- **Operating system:** Microsoft Windows XP®, Windows 7® 32/64-bit, Windows 8/8.1® 32/64-bit
- **RAM:** Minimum 2 GB, due to .NET requirement
- **Hard disk space:** 1 GB of hard disk space should be available to allow collection of historical data
- **Backup:** External backup drive, such as an Iomega or SyQuest Cartridge Hard Disk for backup and history storage.

- **Video:** VGA (640 x 480) at 256 colors minimum, 800 x 600 High color (16 bits) recommended, 1024 x 768 High color supported. True color (24 bits) is also supported. If displaying subscriber images, High color (16 bits) or True color (24 bits) should be used.
- **Modem:** Optional V.32bis (14.4), V.34 (33.8), or V.90 (56.6) modem for remote access and pager dial-out. If modem is external an additional serial port is required.
- **Sound:** Any Windows compatible sound system. One set of computer speakers per computer.
- **Printer:** Parallel or network printers.
- **Additional serial ports (if needed):** Any multi-port board fully supported by Windows. A four-port ISA serial port card made by Digiboard, model AccelePort Xe, part number 76000035. Required four-port cable for DB25, part number 76000008. Digiboard also makes eight- and sixteen-port solutions. They may be contacted at www.digiboard.com.

Databases

- **Alarm reports:** Each alarm is saved as a record containing subscriber data, time and date of alarm, acknowledgment and silence times, responding officer, problem description, and action taken. The alarm map can be reproduced and the location text is displayed.
- **History:** A complete chronological history of all system actions, tests, and alarms is recorded.
- **Operators:** File of those authorized to use the Security Escort system.
- **Subscriber:** Complete record of all subscriber data and current status, low battery, and last test date and time.
- **Transponders:** System configuration containing all installed equipment and system interrelationships.

Other Specifications

- **Temperature range**: 0 ºC to +40 ºC (+32 ºF to +105 ºF)
- **Primary power:** 120 V AC 900 W (two computers, two monitors and one printer).
- **Backup power:** 1200 V A UPS per computer will provide 45 minutes to one hour backup. System should also be backed up by an emergency generator for extended blackouts (can be shared with other emergency equipment).
- **Pager:** Pager support is included and selected troubles can be automatically sent to a service pager.

2.2 SE3 subscriber transmitter

Features

- Alerts Central Console of user’s name and location immediately on alarm.
- Post-alarm tracking, alarm map recall, and more.
- Allows user to test from anywhere within the protected area.
- Internal antenna.
- Four-year battery life, field replaceable.
- Key-chain attachment.

– Low battery indication at Central Console.
– Optional silent alarm.

Description
The SE3 subscriber transmitter contains a unique code which is associated with the subscriber at the time the transmitter is assigned. When the subscriber generates an alarm, this code is sent to the Central Console. The Central Console graphically displays the subscriber's location on a map along with the subscriber's picture, his or her name, and address.

Transmitting an alarm
In the event of an emergency, the user simply presses and holds the alarm buttons to produce an alarm. Depending on the installed options, when an alarm is generated within approximately two seconds, the sounders in any nearby receivers will be activated as well as the strobes and sirens connected to nearby alert units. The alarm signal is transmitted to the receivers which in turn relay the alarm signal to the transponder and along to the Central Console. The Central Console then graphically displays the subscriber's location along with the subscriber's name, vital information (such as a medical condition or disability) and a picture of the subscriber. Also, once an alarm is initiated, the transmitter commences its auto-tracking feature.

Auto-tracking
During an alarm, the transmitter automatically resends the alarm signal every few seconds, constantly updating the Central Console of the subscriber's location.

Testing
The test mode allows a subscriber to test their transmitter anywhere in the protected area. When the user is indoors in sight of an indoor receiver, or outdoors in sight of a strobe, pressing the buttons in sequence performs a test. If the test is successful, a small green light will flash on the indoor receiver, or the strobe will flash briefly. There will be no response at all if the test fails. If the test fails, the user should contact the Security office as soon as possible.
Every successful test is recorded in the **Subscriber Database** in the Central Console software and optionally printed on the hardcopy printer. The **Subscriber Database** contains all of the information relating to each subscriber, including the date and time of the most recent test transmission. It is possible to search the **Subscriber Database** for individuals who have not performed tests for a specified period of time.

Low battery reporting
When the transmitter is tested, a special "low battery" message is included in the transmission to the Central Console if the transmitter's battery is in need of replacing. Also, the system will not give a visual or audible response during a test, indicating that the transmitter requires service. Low battery alerts are logged at the Central Console.

Available models
There are two SE3 models available:
– User transmitter: This is the standard transmitter used by all system subscribers.
– Security transmitter: This is the same as the standard transmitter except the transmitter does not emit an audible tone when activated. This transmitter is normally distributed to Security personnel.

2.3 SE2 personnel transmitter

Features

- Personal duress alarm transmitter.
- Man-down alarm.
- Lanyard pull alarm (optional).
- Allows user to test from anywhere within the protected area.
- Notifies Central Console of user's name and location immediately on alarm.
- Post-alarm and supervision tracking, alarm map recall, and more.
- Internal antenna.
- User replaceable battery with four-year life.
- Belt clip attachment.
- Optional silent manual alarm.
- Low battery indication.
- Optional holster for common security belt sizes.

Description

The SE2 personnel transmitter contains a unique code which is associated with the user at the time the transmitter is assigned. When the user generates an alarm, this code is sent to the Central Console. The Central Console graphically displays the user's location on a map along with the user's picture, and his or her name, and any other necessary information.

Transmitting an alarm

There are three ways in which an alarm may be generated, depending on the features enabled on the transmitter. The types of alarms are as follows:

- **Manual duress alarm:** An alarm can be initiated by pressing the large button on the transmitter.
- **Man-down alarm:** The transmitter will transmit an alarm to the Central Console if it is tipped 60° from upright.
- **Lanyard pull:** A cord connected to the pin inserted in the base of the transmitter can be looped around a utility belt and if the pin is removed from the transmitter (such as when the transmitter is pulled away from the belt), the transmitter will immediately go into alarm.

Auto-tracking feature
During an alarm, the transmitter automatically resends the alarm signal every few seconds constantly updating the Central Console of the user's location.

Supervision tracking
With supervision tracking enabled, the transmitter will send a tracking signal to the Central Console constantly updating the user's location.

Testing
The test mode allows a user to test their transmitter anywhere in the protected area. When the user is indoors, in sight of an indoor receiver, or outdoors, in sight of a strobe, pressing the manual test button performs a test. If the test is successful, a small green light will flash on the indoor receiver, or the strobe will flash briefly. There will be no response at all if the test fails. If the test fails, the user should contact the Security office as soon as possible. When the transmitter is tested, a special "low battery" message is included in the transmission to Central Console if the transmitter's battery is in need of replacing. Every successful test is recorded in the **Subscriber Database** in the Central Console software and optionally printed on the hardcopy printer. The **Subscriber Database** contains all of the information relating to each subscriber, including the date and time of the most recent test transmission. It is possible to search the **Subscriber Database** for individuals who have not performed tests for a specified period of time.

2.4 SE3401 asset tracking transmitter

Features
- Alerts Central Console of Transmitter's ID and location immediately on alarm.
- Available post-alarm tracking, alarm map recall, and more.
- Internal antenna.
- Two-year battery life.
- Can be mounted virtually anywhere on virtually anything.
- Low battery indication at Central Console.
- Includes mounting plate.

Description
The SE3401 Point Tracking Transmitter contains a unique code which is associated with an asset at the time the Transmitter is assigned. When an alarm is generated, this code is sent to the Central Console, which graphically displays the asset's location on a map along with a picture of the asset and any other necessary information.

Installation
The SE3401 can be configured to monitor magnetic or dry external contacts. When mounted with an external magnet, the SE3401 is mounted on the asset and the magnet is mounted on an opposite surface (such as a wall). When mounted with external contacts, the SE3401 can be mounted anywhere on the asset and connects to the contact by two wires connected to the terminals inside the Transmitter and an end-of-line resistor.

Transmitting an Alarm
Depending on the installed options, when an alarm is generated within approximately two seconds, the sounders in any nearby Receivers could be activated as well as the Strobes and Sirens connected to nearby Alert Units. The alarm signal is transmitted to the Receivers which in turn relay the alarm signal to the Transponder and along to the Central Console. The Central Console graphically displays the Transmitter's location along with the asset's description and a picture of the asset. Also, once an alarm is initiated, the Transmitter commences its Auto-Tracking feature.

Auto Tracking Feature
Once an alarm has been initiated (such as when the Transmitter has been moved away from the magnet) the Auto-Tracking feature will begin. The Transmitter will send a signal back to the Central Console every few seconds updating its location for several minutes. To reset the Transmitter after an alarm has been initiated, all device conditions (e.g., tamper, loop, magnet) must be reset to normal.

Supervision Feature
The SE3401 Point Tracking Transmitter can also be configured to transmit periodically when there is no other activity to report its status and location to the Central Console.

Low Battery Reporting
When the Transmitter is tested, a special "low battery" message is included in the transmission to the Central Console if the Transmitter's battery is in need of replacing. These low battery alerts are logged at the Central Console.

2.5 RF3401 asset tracking transmitter

Features
- Supervised Sensor Loop (monitors any dry contact device)
- Internal Reed Switch (used with magnet)
- Supervisory Signal Every 65 Minutes
- Complete Status, including Battery and Tamper Sent with Every Transmission
- Compatible with all DS RF-TechTM Receivers @304 MHz
- Factory Programmed Transmitter ID for Quick and Simple Transmitter Enrollment

– Installer (or user) Replaceable Lithium Battery
– Quick Install Mounting Base Plate Included
– Cover Tamper

Description

The RF3401 Point Transmitter features a supervised sensor loop and a magnetic reed switch. Use the supervised sensor loop to monitor any device with a dry contact output. When used with an external magnet assembly the RF3401 reed switch allows for quick and easy installation on doors and windows.

2.6 SE88 panic transmitter

Features

– Can be worn like a watch, pendant or mounted to a permanent location
– Once activated, sends immediate notification of wearer's identity and location
– Water resistant

Description

The SE88 Security Escort Watch/Pendant Panic Transmitter is designed to work with the Security Escort System. Once activated, the wearer's identity and location is sent to the security office. The SE88 may be worn like a watch, around the neck like a pendant or even mounted to a stationary location with a mounting bracket (optional accessories, please order separately). It is ideal for use in elder care or assisted living facilities where immediate emergency notification is required.

Transmitting an Alarm

– In the event of an emergency, the user simply presses and holds the alarm buttons to produce an alarm. Transmittal will vary with different options. Generally, within two seconds of an alarm being generated, sounders in Receivers and Strobes or Sirens connected to Alert Units will activate.
– The alarm signal transmits to the Receivers. The Receivers relay the alarm signal to the Transponder and to the Central Console.
– The Central Console displays the user’s location, picture, name, and vital information (such as a medical condition or disability).

Auto-Tracking Feature

– During an alarm, the Transmitter automatically resends the alarm signal every few seconds constantly updating the Central Console of the user's location.

Testing

– The Test Mode allows a user to test his or her Transmitter anywhere in the protected area. When the user is indoors in sight of an Indoor Receiver, or outdoors in sight of a Strobe, pressing the buttons in sequence performs a test. If the test is successful, a small green light will flash on the indoor Receiver, or the Strobe will flash briefly. There will be no response at all if the test fails. If the test fails, the user should contact the Security Office as soon as possible.
– Every successful test is recorded in the Subscriber Database in the Central Console Software and optionally printed on the hardcopy printer. The Subscriber Database contains all of the information relating to each subscriber, including the date and time of the most recent test transmission. It is possible to search the Subscriber Database for individuals who have not performed tests for a specified period of time.

Low Battery Reporting

– When the Transmitter is tested, a special "low battery" message is included in the transmission to Central Console if the Transmitter's battery is in need of replacing. Also, the system will not give a visual or audible response during a test, indicating that the Transmitter requires service. Low battery alerts are logged at the Central Console.

2.7 SEFD1 transmitter

Calls for Help Even When You CannotCalls for Help Even When You Cannot

The SEFD1 Fall Detector and Personal Help Button provides assistance that no other personal Help Button can offer. The device alerts your emergency monitoring service *automatically* when it detects a fall, even if you are unable to push the Help Button on the device.

The SEFD1 is designed to work in and immediately around your home or facility. The device must be close enough to a receiver for a help signal to be received. The coverage area of the device will vary from one location to another. It is important for you to know the effective range of your device.

The SEFD1 is designed to detect falls that meet certain criteria. It may not detect every fall, especially slight falls that are generally not disabling. The SEFD1 Fall Detector device may also generate a fall alarm when you have not fallen. For example, if the device drops on the floor, it may alert the monitoring center that you have fallen.

Operation

The SEFD1 device transmits three conditions:

– Push Button (Help Button)
– Fall
– Low Battery

2.8 EA102 receiver

Features

- Receives Transmitter alarms and tests, and relays the information to the Transponder.
- Built-in self testing through Buddy Check feature.
- Indoor and outdoor security enclosures available.
- Indoor enclosure provides confirmation of successful Transmitter test. (Outdoor enclosures use other type of signaling device, such as a Horn/Strobe.)
- Indoor Receivers provide local sounders in alarm events.

Description

The Receivers are located throughout the protected area, including building interiors.
Each Receiver contains a radio receiver to detect the transmissions from Transmitters, and a microcomputer to decode and interpret the received test and alarm messages. In addition, the microcomputer monitors tampering and other problems, and reports such conditions to the Transponder.
Each Receiver contains an internal self-contained sounder. These sounders are optionally activated if the Receiver has detected an alarm transmission.
Indoor Receivers are typically mounted on inside walls and are housed in small beige, rectangular units. Indoor Receivers have one red and one green light. The green light is used to indicate a successful test of a Transmitter; the red light is only illuminated during certain system tests and during alarms.
Outdoor Receivers are contained in small weatherproof enclosures typically mounted on the sides of buildings and on light posts. Outdoor Receivers do not have the visible red and green LED’s. Outdoors, the strobe lights connected to the Alert Units flash to acknowledge a successful test.

Function During an Alarm

In the event of an alarm, the Receivers detect an alarm signal from a Transmitter and send this information to the Transponder. The Transponder forwards this information the Central Console where, using the reported information from all the Receivers that detected the signal, the location of the transmission is graphically displayed on the Alarm Map.

Buddy Check

In addition to its radio receiver, each Receiver also contains a transmitter functionally similar to the hand held Transmitters. This transmitter can be commanded by the Central Console to transmit a test message to other nearby Receivers. This Buddy Checking is performed periodically to verify that the Receivers are functioning satisfactorily. Results of the Buddy Check are compared with the results of earlier Buddy Checks, and any changes in a Receiver’s sensitivity are reported to the Central Console where this information is stored in a system database.

2.9 EA500 transponder

Features

- Relays alarm and test signals from the Receiver to the Central Console.
- Can support a combined total of 64 Receivers and Alert Units.
- AC powered with battery backup for all Receivers.
- Can provide power to SE485 Interface and/or Spread Spectrum Radio.
- Available in a large or small indoor enclosure.
- Monitors Receivers and Alert Units 10 times per second for alarms, tests, tamper notification, and power loss.

Description

The Transponder is a device controller for up to 64 devices -- any combination of Receivers and Alert Units. Its primary function is to monitor the Receivers and Alert Units and report conditions and events to the Central Console via either wire or ProxLink radios. It also provides power output to certain devices.

Installation

The Transponder can be mounted in one of two different sized enclosures. It is always mounted indoors. The devices are connected to the Transponder by means of eight four-wire Multiplex Busses, two wires for power and two wires for data. Each bus is capable of supporting up to eight devices. A Security Escort System supports up to 255 Transponders.

Configuration

Each Receiver and Alert Unit is identified to its Transponder by a Multiplex Address which is set during system installation using a multi-position switch on the Receiver or Alert Unit circuit board. Transponders communicate on the data bus with individual Multiplex devices by issuing commands, which contain the Receiver or Alert Unit’s Multiplex Address.

Setup and Testing

Each Transponder and the devices connected to it are set up and can be tested remotely from the Central Console. Also, each Transponder reports any problems, such as low battery, immediately upon detecting them.

Function During an Alarm

When a Receiver or Alert Unit detects an alarm, it goes into an “Off Normal” state. To quickly locate any devices which might be in the “Off Normal” state, the Transponder issues global commands (which are interpreted simultaneously by all of its devices) approximately 10 times per second. These global commands are followed by commands to specific devices to determine the nature of the “Off Normal” condition and, in the case of an alarm (or test), to obtain the Transmitter Identification Number, Transmitter battery condition, and received signal strength. This information is then sent to the Central Console, by either wire or through ProxLink radios, where it is used to graphically display the identity of the subscriber transmitting the alarm and to determine the subscriber’s location.

2.10 EA120 alert unit

Features

- Provides output for alarm annunciation through the Siren/Strobe or other third party switched device.
- Provides output to Siren/Strobe to indicate a successful Transmitter test.
- Indoor and Outdoor enclosures available.
- AC powered with battery backup.
- Activated on command from the Central Station through the Transponder.
- Reports tampering, AC power loss, backup battery power to the Transponder, and output status.

Description

An Alert Unit is a control module that communicates with the Transponder on the MUX Bus. In most installations, it is used to activate Siren/Strobe units or other switched devices in the event of an alarm. The Alert Unit also reports tampering, AC power loss, and backup battery level to the Transponder.

Installation

The Alert Unit may be housed in either a metal indoor enclosure or an outdoor enclosure (similar to the Outdoor Receiver enclosure), depending on the application. The Strobe/Siren units are always mounted in outdoor locations.

Function

The Alert Unit has backup battery power in addition to AC power. The Alert Unit Driver contains a microprocessor that communicates with the Transponder for Strobe and Siren commands, status reports, and trouble indications. The troubles monitored are “Tamper”, “Loss of AC Power”, and “Low Battery”.

Test Acknowledgment

In addition to the function of attracting attention in the event of an emergency, the Strobe unit is used to acknowledge a successful test of a Transmitter. The Alert Unit can be configured to cause a Siren to emit a short tone and the strobe to flash for a successful Transmitter test.

Function During an Alarm

In the event of an alarm, the Alert Unit receives a signal from the Transponder and begins powering the Siren/Strobe (or other switched device). The Siren/Strobe will be active until the alarm is restored at the Central Console.

3 Equipment estimation, location accuracy and receiver location

A Security Escort system installation consists of three major steps:

1. the pre-bid equipment estimation,
2. the pre-construction coverage verification survey, and
3. the post construction setup.

The Security Escort receivers work effectively in a wide variety of installations and can be placed with confidence provided these installation requirements are met. Therefore, at the pre-bid stage, it is acceptable to estimate the required equipment. To ensure proper coverage after proposal acceptance, potential receiver locations can be verified using a standard receiver in test mode or the portable test receiver before construction begins.

3.1 Location accuracy

The Security Escort system provides quick response to a duress call. Its intent is to dispatch a responding individual to an area without additional delay to their response to that duress call.

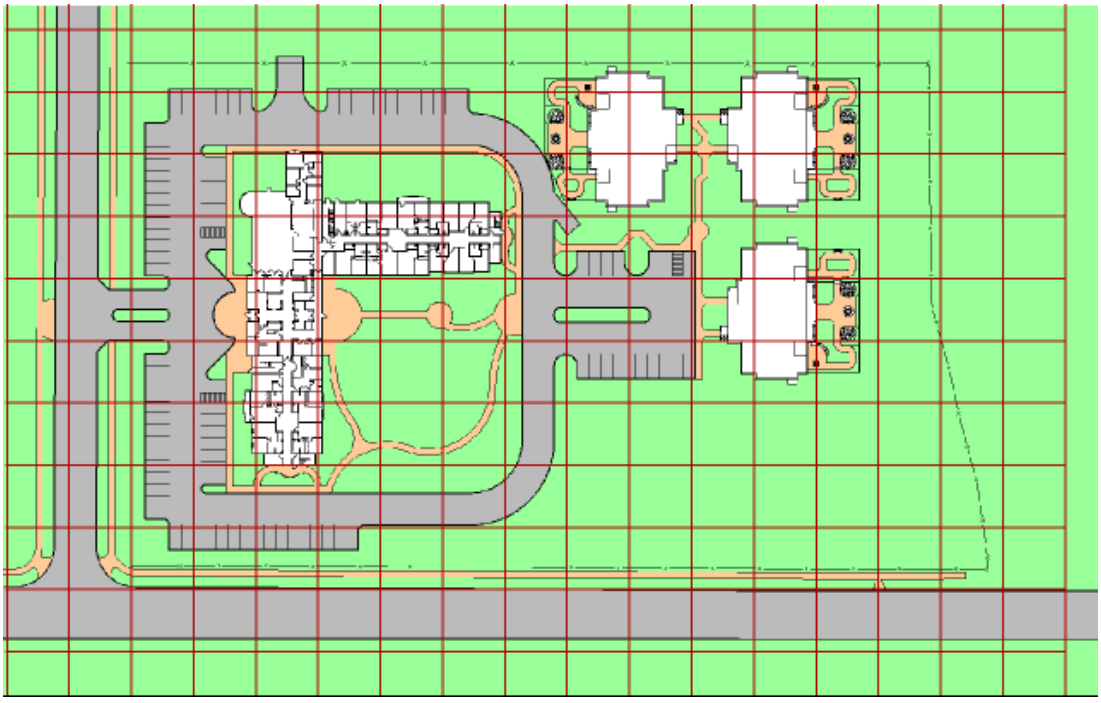


Figure 3.1: System Block Diagram

The Security Escort system uses radio frequency (RF) for alarm transmissions. This is significant because it prevents normal construction from blocking the signal and helps to eliminate dead spots where the alarm could not be heard. The fact that RF energy passes through normal construction prevents Security Escort from locating an alarm with 100% certainty to a specific side of a wall. Alarms originating at or near building walls will typically be indicated within 7.5 m (25 ft) of the actual location. However, there may be times when the computed location may appear to be on the other side of the wall.

The Security Escort system was designed to provide a computed alarm location typically within 7.5 m (25 ft) of the actual location when indoors, and a computed alarm location typically within 15 m (50 ft) of the actual location outdoors. Any deviation from the following installation guidelines will degrade the computed location accuracy. Therefore, to achieve accuracy, the following installation guidelines must be adhered to.

3.2 Pre-bid equipment estimation

The pre-bid equipment estimation is performed prior to bidding the installation. At this point, it must be determined what type of coverage is desired, and where the coverage will be required. For example, the amount of equipment required for a full-coverage (indoor and outdoor) system in a multi-building application is greater than an installation that requires outdoor only coverage. The customer should be consulted, and the areas of most concern should be given special consideration.

3.2.1 Initial equipment estimate

Number of indoor receivers

To estimate the number of indoor receivers, assume the receivers will be placed on a grid with a maximum spacing of 25 m (80 ft) between receivers for standard construction. In multi-floor applications, the receivers on each floor must be placed directly above the receivers on the floor below (this is required for proper floor-to-floor location).

To estimate the number of indoor receivers, first read Indoor receiver installation. Assume the receivers are placed on a grid with a maximum spacing of 25 m (80 ft) between receivers for standard construction. In multi-floor applications the receivers on each floor must be placed directly above the receivers on the floor below (this is required for proper floor-to-floor location).

For example, to determine the number of receivers required to protect a building of standard construction of 60 m x 30 m (200 ft x 100 ft) and four floors:

1. To determine the number of receivers in each direction, divide each dimension of the building by 25 m (80 ft), drop the remainder, and add 1. For example:
   - 60 m/25 m = 2.4, becomes 2, add 1 = 3
     (200 ft/80 ft = 2.5, becomes 2, add 1 = 3)
   - 30 m/25 m =1.2, becomes 1, add 1 = 2
     (100 ft/80 ft =1.25, becomes 1, add 1 = 2)
2. To determine the number of receivers required per floor, multiply the number of receivers in one direction by the number of receivers in the other direction.
   (3 x 2 = **6**) 6 receivers per floor.
3. To determine the total number of receivers, multiply the number of receivers per floor by the number of floors.
   (6 x 4 = **24**) 24 receivers for the building.

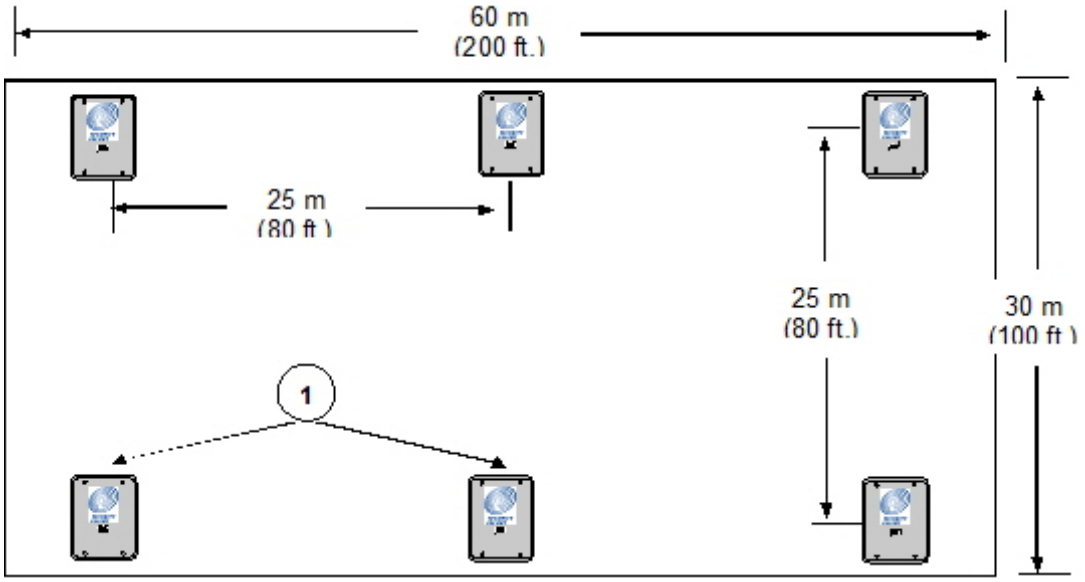
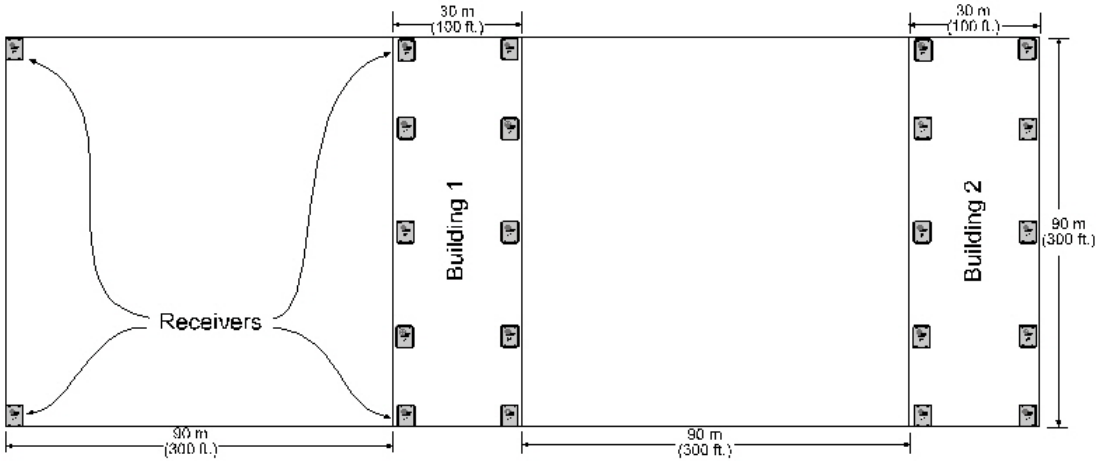


Figure 3.2: Determining the Number of Indoor Receivers Required

1	Receivers (6)		

Each floor would require 6 receivers, resulting in a total of 24 receivers to protect this building.
For the best location accuracy, consistent receiver spacing is important. Do not place receivers significantly closer in one section of a building than another section.

Number of outdoor receivers



To estimate the number of receivers, first read Outdoor receiver installation. Assume a maximum receiver spacing of 90 m (300 ft) between receivers, in both directions, for receivers that are not within 30 m (100 ft) of a building with inside coverage. Receivers within 30 m (100 ft) of a building should be spaced the same as receivers in the building (spacing the outside receivers at a somewhat larger spacing is acceptable in most cases).

An outside area directly between two buildings with inside protection will need no additional receivers if the buildings are 90 m (300 ft) or less apart. If the buildings are more than 90 m (300 ft) apart the outside receivers should be evenly spaced between the buildings. Make sure the standard 90 m (300 ft) spacing is not exceeded. For spacing outside adjacent to a covered building, start the 90 m (300 ft) spacing at the building wall.

Allowance for special coverage requirements
For purposes of the bid, the number of receivers estimated above should be raised by 5% to allow for special coverage considerations and RF problem areas.

Number of transponders
Assume one transponder per building for indoor installations. If wiring can be run from other buildings or from outdoor receivers, they may be connected to one transponder. Never exceed the total number of 64 devices (receivers and alert units) per transponder. All outside wiring must be under ground, or in metal conduit.

Number of receivers and alert units per bus
For transponders, each bus can handle 8 receivers and alert units. However, it is a good idea to leave some addresses available on each bus to allow for future expansion. For systems with a high number of supervised transmitters, see Transponder wiring notes.

Bus wire
The multiplex bus for transponder should be wired with 4 conductor 18 gauge (1.2 mm) wire. The wire should not be paired or shielded. In the United States this is the same as fire system wire, except it should not be red.

Number of alert units
The number of alert units will be determined by each system's requirements. In general, enough alert units should be installed to be heard and seen from all outdoor locations of protection. Remember that even in a silent system, alert units can be used outside to provide test feedback. Horn/strobe units should be mounted in predictable locations to make them easy to identify by subscribers. Alert units are not required indoors because the indoor receiver provides alarm and test feedback. Each transponder will drive one siren and one strobe if they are less than 15 m (50 ft) from the transponder.
It is a good idea for each protected parking lot to have a siren/strobe near it.

3.3 Pre-construction coverage verification survey

The pre-construction coverage verification survey is performed after the bid is accepted and before construction begins. It is done to determine the location of each receiver. Each receiver location should be checked using a standard receiver in the test mode.

3.3.1 Verify each potential receiver location

Using a receiver in "receiver spacing" mode
"Receiver spacing" mode is enabled with jumper P5 in place (jumper P4 removed) on a receiver (see the *EA102 Receiver Installation Instructions*).
This mode is exactly the same as the "test" mode, except that only transmissions with an adequate receive margin are sounded. This indicates the maximum acceptable spacing of receivers. Use the following procedure to test the spacing of receivers:

1. Mount the first receiver.
2. Put jumpers P1, P2, P3, and P5 in place, and remove all other jumpers. Power the receiver from a or 12 VDC source.
3. Take the second receiver and a transmitter a distance away from the first receiver.
4. Activate the transmitter.
5. If receiver 1 sounds the test beep, receiver 2 is within range. Repeat this test until receiver 1 no longer sounds the test beeps. Move back to the last location where receiver 1 received the test beeps. This location marks the maximum spacing between receivers. The distance between receivers should not exceed 25 m (80 ft) indoors and 90 m (300 ft) outdoors. Mount receiver 2 at this location or closer to receiver 1.

Notice!
Do not use the “test” mode (jumper P4) to determine receiver spacing.

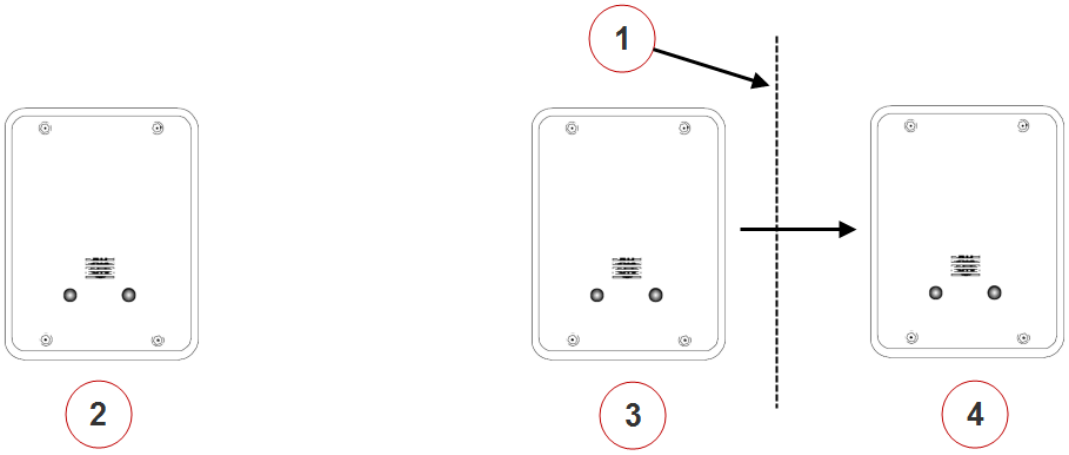


Figure 3.3: Receiver Spacing

1	Receiver 1 stops sounding the test beeps when receiver 2 is moved past this point	3	Receiver 2 at maximum range
2	Receiver 1	4	Receiver 2 beyond maximum range

Using a transponder, receivers, and laptop computer to determine receiver location

Notice!
System software and an area map must be installed on a laptop computer to use this method.

A transponder with long multiplex wires connected to receivers can be used to see actual alarm location before the receivers are placed. Place the receivers in the proposed locations wired back to the transponder. Program the receivers with their locations in the **Transponder Database**. Using the maintenance transmitter and the maintenance alarm database, activate alarm transmissions within the area surrounded by the temporarily placed receivers. Verify that the location accuracy is acceptable at all points of concern. If not acceptable move the

receivers, update the receiver location in the **Transponder Database**, and retest. Do not test outside of the last receiver in any direction, as this gives incorrect locations. Repeat this test in all areas of different construction and concern at the site.

3.3.2 Indoor receiver installation

- Indoor receivers must be mounted in a evenly spaced grid no more than 25 m (80 ft) apart.
- Indoor receivers must be mounted 1.5 to 1.8 m (5 ft to 6 ft) above the floor. This is true even if this is a single story building. Do not mount receivers above the ceiling or in roof rafters.
- In multistory buildings, the receivers must be mounted directly above the receivers on the floor below. The same number of receivers must be used on each floor level. If you meet all of the indoor installation guidelines, you can expect the computed location to indicate the correct floor about 95% of the time.
- Receivers must not be mounted within 30 cm (1 ft) of any metal object, including wire mesh, metal foil, metal pipe and HVAC ducting in walls.
- Take care that large metal objects do not shield a receiver from a protected area. For example metal staircases, metal food serving lines, metal walls, lead lined walls, metal roofs, wire mesh in walls, walk-in freezers and refrigerators.

For the best indoor and outdoor location or an indoor only system

- Mount the indoor receivers on the recommended 25 m (80 ft) grid, with the last row of indoor receivers on the outside wall of the building. Do this even if the building is less than 25 m (80 ft) wide or long.
- There should be a receiver at each outside corner of a building.

Handling two protected buildings sharing a common wall with floor levels that do not match

- Ask the customer which building has areas of greater concern and favor the recommended mounting heights in that building.
- The recommended 25 m (80 ft) maximum indoor spacing grid should be maintained throughout both buildings as if the wall in question was not there. Mounting heights only for those receivers at or near (within 6 m [20 ft]) the wall in question should be affected. Mounting heights for all other receivers in the buildings must follow the indoor recommendation. Mark the recommended mounting height for receivers on the higher floor level and also mark the recommended mounting height for receivers on the lower floor level. Mount the receiver at its normal grid location midway between these two heights, but not above the ceiling level of the lower floor.

3.3.3 Outdoor receiver installation

- Outdoor receivers must be mounted in a evenly spaced grid no more than 90 m (300 ft) apart.
- Outdoor receivers must be mounted 3 m (10 ft) above the ground.
- Receivers must not be mounted within 30 cm (1 ft) of any metal object, including fences, metal walls and walls with wire mesh. If a receiver is mounted on a metal fence, that fence should be grounded (not floating or insulated from ground) and the receiver should be spaced 30 cm (1 ft) from the fence and 3 m (10 ft) above the ground.

- Take care that large metal objects do not shield a receiver from a protected area. For example; metal fences, metal staircases, metal buildings, power transformers and metal roofs.
- Receiver locations should be below building overhangs and eaves as these can shield the areas below them.
- Receivers should have a clear line of sight of the protected area. Therefore, take care where the ground is hilly or uneven, that there are no areas and low spots where several receivers can't hear the signal.

Transition areas between indoor and outdoor areas

- An outside area directly between two buildings with complete indoor protection will need no additional receivers between the buildings, if they are 90 m (300 ft) or less apart.
- When protecting an outside area directly between two buildings with complete indoor protection, and they are more than 90 m (300 ft) apart, place a row of outside receivers evenly spaced between the buildings. Make sure the receiver row does not exceed the standard 90 m (300 ft) spacing from the buildings. The spacing between receivers in that row should be about the same as the spacing for the receivers in the buildings.
- Indoor receivers should be no more than 25 m (80 ft) apart and outdoor receivers should be no more that 90 m (300 ft) apart. Both of these recommendations work well in their respective areas. However, if a building is adjacent to an outdoor area, that building will have a greater density of receivers and, therefore, has a tendency to pull the computed location towards it. To counteract the building tendency to pull the location, consider the following special cases:
  - If the outdoor area adjacent to the building is wide open and the customer is not concerned about reduced location accuracy in this area, then nothing special needs to be done. Follow the normal indoor and outdoor recommendations.
  - The building is near the boundary of the protected area, with or without a fence at the boundary. The receivers in the building should be placed at the recommended 25 m (80 ft) spacing. The receivers at the boundary of the protected area near the building should be spaced about the same as those in the building, approximating the same grid as used in the building.
  - The building is adjacent to a large protected outdoor area that extends for more than 90 m (300 ft) from the building. The receivers in the building should be placed at the recommended 25 m (80 ft) spacing. The receivers in the large protected outdoor area should be placed on the normal 90 m (300 ft) grid except for the first row of receivers adjacent to the building. This first row of outdoor receivers in the transition area should "split the difference" between the indoor and outdoor spacing at about 60 m (200 ft).

Boundary areas at the outer edge of the protected area

The system cannot locate an alarm past the last receiver at the boundary of the protected area. Therefore, the last row of receivers must be at or past the end of the protected area.

4 System wiring

4.1 General guidelines

After the site survey (and special pre-construction verifications) has been completed, the wiring can be run between the proposed locations of the system components and the Central Console. See specific installation instructions accompanying each component for wiring details.
The following table indicates the specifications for the wiring:

Application		Diagram Ref	Gauge	Conductors	Maximum Distance	Notes
From	To					
Transponder	Transformer	1	1.5 mm (16 AWG)	2	15 m (50 ft)	Standard lamp cord
	Alert Unit	2	1.2 mm (18 AWG)	4	900 m (3000 ft) per bus	Solid, not twisted, not shielded
	Receiver	2	1.2 mm (18 AWG)	4	900 m (3000 ft) per bus	Solid, not twisted, not shielded
	SE485	3	0.5 mm (24 AWG)	4 wire, 2 twisted pair	See Transponder – SE485 Wiring table.	**IMPORTANT!** Must be twisted pair, not shielded. CAT5 cable preferred.
	Siren/Strobe	4	1.2 mm (18 AWG)	4	15 m (50 ft)	Solid, not twisted, not shielded
Alert Unit	Transformer	5	1.5 mm (16 AWG)	2	15 m (50 ft)	Standard lamp cord
	Siren/Strobe	6	1.5 mm (18 AWG)	4	15 m (50 ft)	Solid, not twisted, not shielded

Table 4.1: Wiring Guidelines

4.1.1 Transponder - SE485 wiring table

Number of Transponders	Maximum Wire Length
1 to 4	6100 m (20000 ft)
8	3050 m (10000 ft)

Number of Transponders	Maximum Wire Length
12	1525 m (5000 ft)
16	900 m (3000 ft)

Table 4.2: Transponder – SE485 Wiring Table

4.1.2 Observe established standards

Install cable according to local code requirements. In the USA, refer to *the National Electrical Code Standards*, located *in Chapter 8 Article 800* of the *National Electrical Code*, and applicable local and regional codes.

4.2 Component wiring guidelines

4.2.1 General wiring diagram

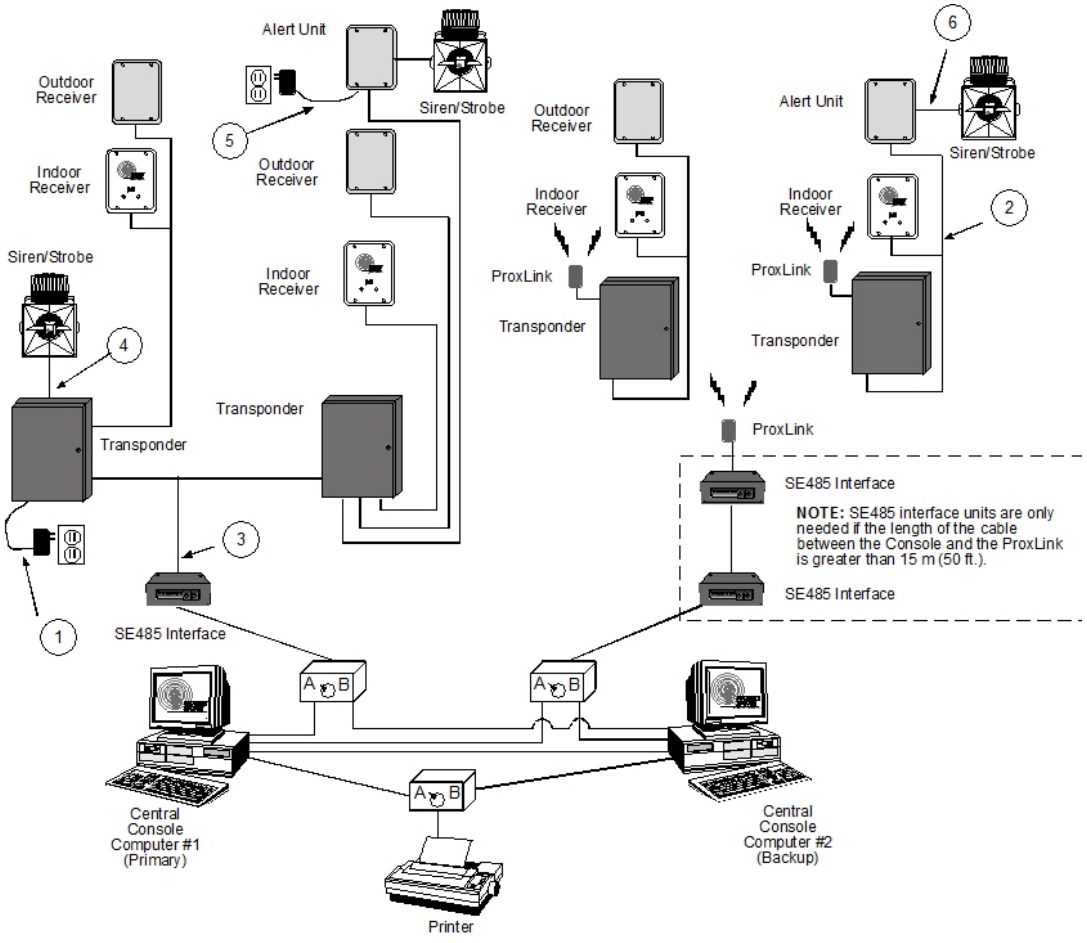
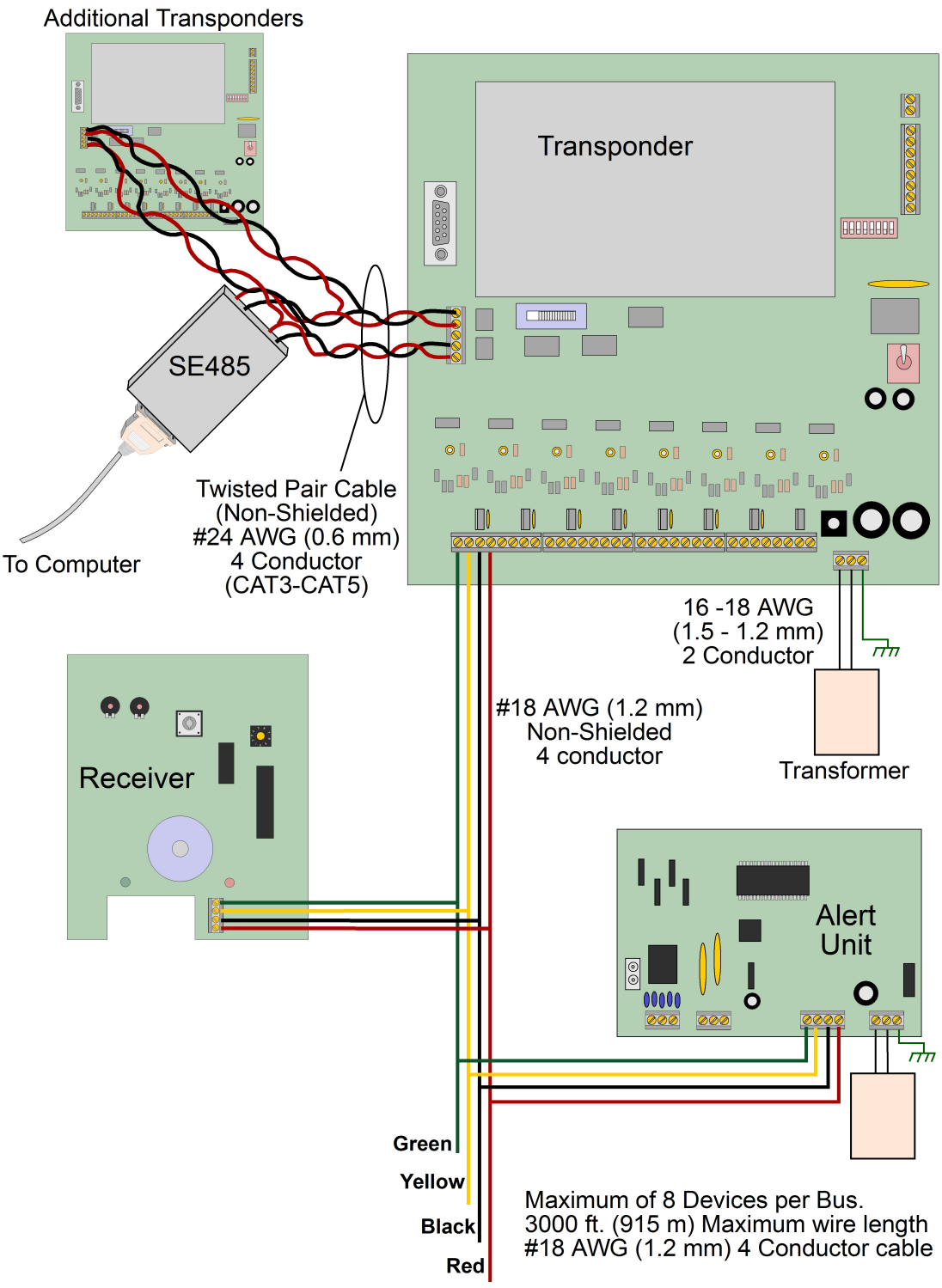


Figure 4.1: General Wiring Diagram


Additional Transponders
Transponder
SE485
To Computer
Twisted Pair Cable
(Non-Shielded)
#24 AWG (0.6 mm)
4 Conductor
(CAT3-CAT5)
16 -18 AWG
(1.5 - 1.2 mm)
2 Conductor
#18 AWG (1.2 mm)
Non-Shielded
4 conductor
Transformer
Receiver
Alert
Unit
Green
Yellow
Black
Red
Maximum of 8 Devices per Bus.
3000 ft. (915 m) Maximum wire length
#18 AWG (1.2 mm) 4 Conductor cable

4.2.2 Transponder information sheet

Transponder Number:		**Transponder Location:**	
Transformer for Transponder Location:			
Breaker Panel Location:		**Breaker Number:**	
Siren/Strobe Output To:			
Keyswitch Monitoring To:			
Bus #0 Locations:			
Point #0:			
Point #1:			
Point #2:			
Point #3:			
Point #4:			
Point #5:			
Point #6:			
Point #7:			
Bus #1 Locations:			
Point #0:			
Point #1:			
Point #2:			
Point #3:			
Point #4:			
Point #5:			
Point #6:			
Point #7:			
Bus #2 Locations:			
Point #0:			
Point #1:			

Point #2:	
Point #3:	
Point #4:	
Point #5:	
Point #6:	
Point #7:	
Bus #3 Locations:	
Point #0:	
Point #1:	
Point #2:	
Point #3:	
Point #4:	
Point #5:	
Point #6:	
Point #7:	
Bus #4 Locations:	
Point #0:	
Point #1:	
Point #2:	
Point #3:	
Point #4:	
Point #5:	
Point #6:	
Point #7:	
Bus #5 Locations:	
Point #0:	
Point #1:	
Point #2:	
Point #3:	
Point #4:	
Point #5:	

Point #6:	
Point #7:	
Bus #6 Locations:	
Point #0:	
Point #1:	
Point #2:	
Point #3:	
Point #4:	
Point #5:	
Point #6:	
Point #7:	
Bus #7 Locations:	
Point #0:	
Point #1:	
Point #2:	
Point #3:	
Point #4:	
Point #5:	
Point #6:	
Point #7:	
Location of Splices:	

4.3 EA500 transponder

4.3.1 General

The EA500 transponder is the Security Escort module that provides communications between the Central Console and the many receivers and alert units throughout the protected area. In addition to its communications functions, it also supplies power to the receivers. Each transponder also includes drivers for a single strobe and siren.

4.3.2 Specifications

Enclosure (AE3):	15 in. W, 20.75 in. H, 4.25 in. D
Hardware Kit:	H500
Temperature Range:	-40° to +149°F (-40° to +65°C)
Power:	18.0 VAC, 50 VA maximum plug-in Transformer for 110 V, 60 Hz Supplies battery backed 12.0 VDC power to Receivers
Power Output:	9V DC used for SE485 or for Proxim radio power
Driver Outputs:	*Strobe*: 500 mA solid state sink, terminal switches to ground in an alarm condition. *Siren*: 500 mA solid state sink, terminal switches to ground in an alarm condition.
Battery Backup:	12 VDC Lead Acid Battery
Multiplex Buses:	8 multiplex drivers, each capable of driving 8 Receivers or Alert Units for a combined total of 64 Receivers and Alert Units per transponder
Comm. Interface:	Selectable SE485 or RS-232
Keyswitch Input:	47k EOL resistor, supervised loop
Compatibility:	*ROM version 4.00 or greater (version shipped with this unit) is compatible with “-304” equipment (e.g., EA102A-304). Version 4.00 or greater is NOT compatible with non “-304” equipment. *ROM versions earlier than 4.00 are compatible with non “-304” equipment.

4.3.3 Mounting

Normally, the enclosures are mounted first and all the wiring run, then the electronics are mounted, wired, and tested.

The enclosures come with their own mounting hardware (H500 Hardware Kit) for mounting the enclosure to a wall and mounting the circuit board to the enclosure.

– Mount the enclosure to the mounting surface.
– Mount the circuit board to the enclosure.

4.3.4 Wiring

Wire the transponder. See wiring diagram on *Set the address, page 37*.

Wiring to receivers and alert units can be home-run (individual), daisy-chain (from device to device), or a combination of both. T-tapping is okay. The recommended cable is 4-conductor, 18 AWG (1.2 mm) fire rated.

Wiring from SE485 to transponders can be home-run (individual), daisy-chain (from device to device), or a combination of both. T-tapping is okay. The recommended cable is 4-conductor, 22 AWG (0.8 mm).

4.3.5 Set the address

Every transponder in the system must have its own address. Set the address on the transponder using the dip switches in the upper-right corner. See figure below.

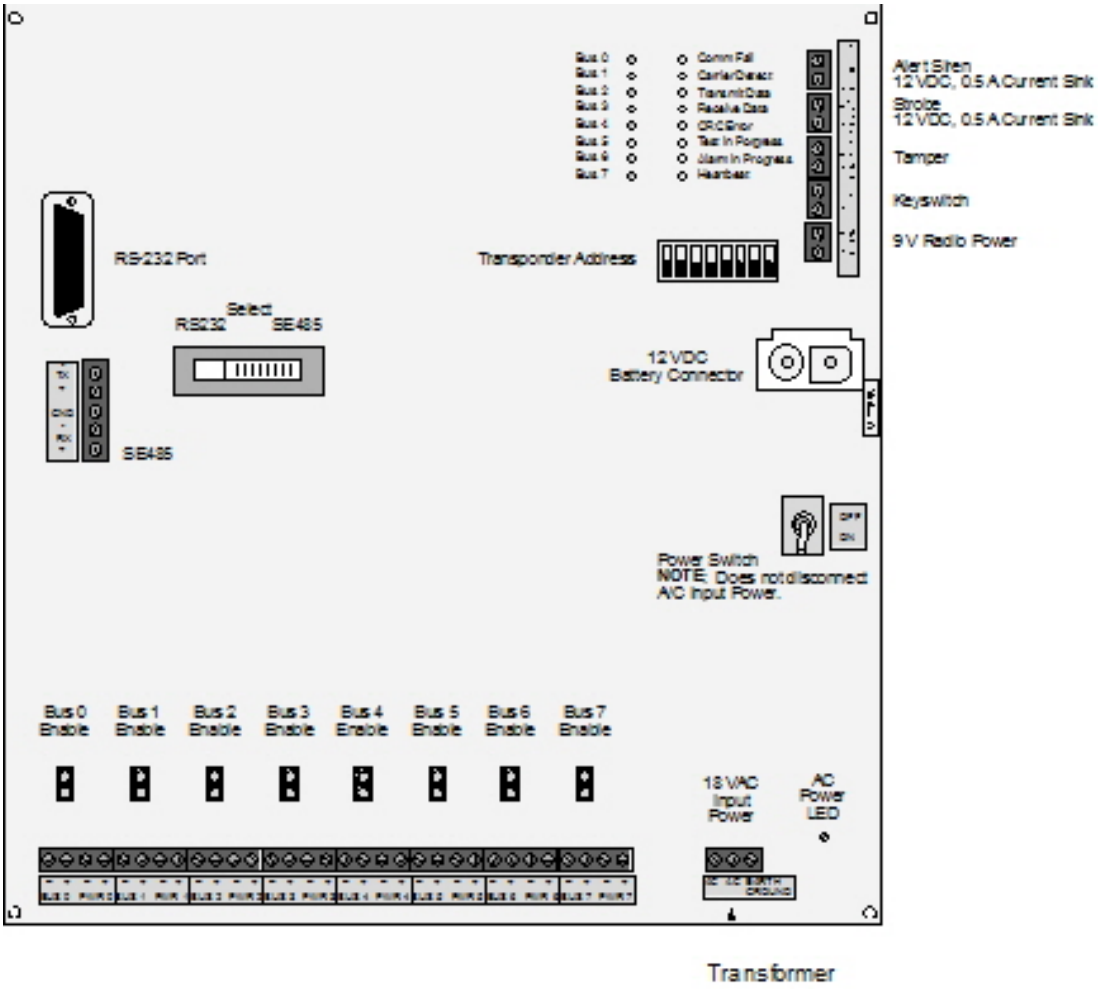


Figure 4.2: Transponder

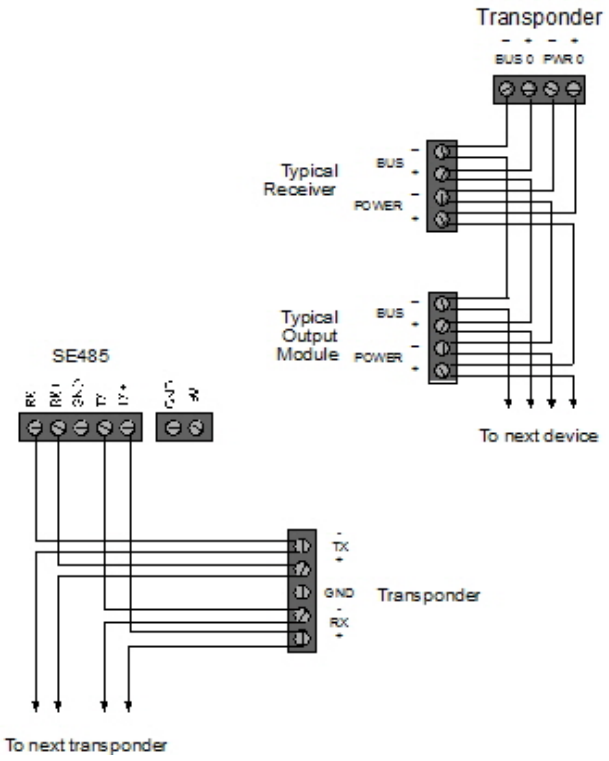


Figure 4.3: Wiring

The figure below shows how to set the dip switches for each possible address.

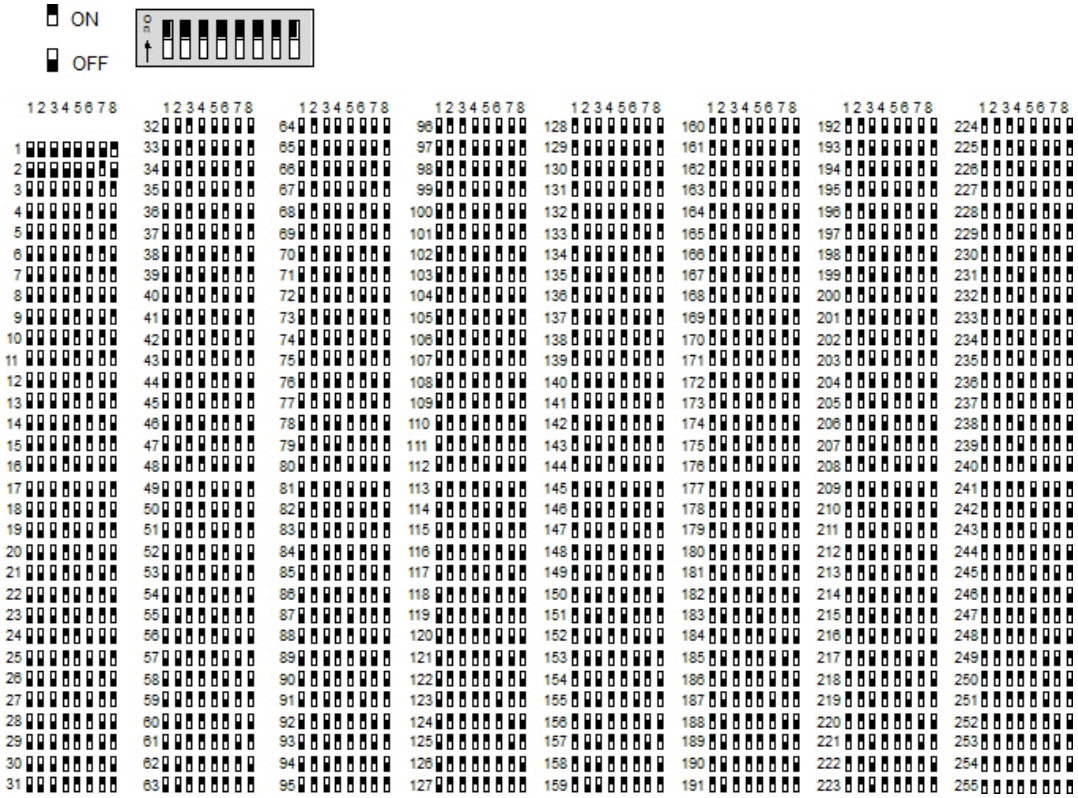


Figure 4.4: Dip switch settings

4.4 EA102A-304 receiver

4.4.1 Specifications

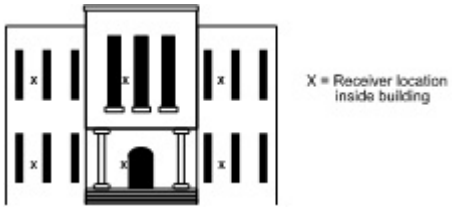
Enclosure	Available in indoor and weatherproof outdoor enclosure
Temperature Range	-40° to + 149°F (-40° to +65°C)
Power	12VDC, 25 mA typical, 55mA with horn sounding
RF Input Frequency	304.000 Mhz
Signal Strength	Measured in 255 steps
Antenna Type	Diversity antennas
Compatibility	SE2x-304 Series and SE4x-304 Series Transmitters; EA500B Transponder with a ROM version 4.00 or greater.

Notice!
The EA102A-304 is compatible only with other “-304” equipment (e.g., the SE2x-304 and the SE4x-304). Also, do NOT install this unit in conjunction with an EA500B transponder with a ROM version earlier than 4.00.

4.4.2 Mounting

Choose a mounting location based upon the previous site survey. The receiver should be mounted as close as possible to the location found with the test receiver. The following is a guideline for receiver mounting and spacing:

Indoor receiver installation
Receiver spacing: Receiver spacing should be no more than 24 m (80 ft) between receivers for standard construction. Range will be dependent upon the construction of the building. For example: a building with hollow drywall walls may support 24 m (80 ft) spacing; a building with steel reinforced concrete may require reduced spacing. It is very important to maintain a consistent spacing as this will ensure optimum signal locating. The more receivers that can detect a transmitted signal, the more accurate the locating will be.
Mounting height: Receivers should be mounted 1.5 to 1.8 m (5 to 6 ft) from the floor. Maintain a consistent mounting height to ensure optimum signal locating. Do not place receivers close to the ceiling; this will cause them to be closer to the floor above, and therefore, reduce the floor to floor location accuracy. It may also be helpful to place the receivers somewhat higher only on the top floor to be covered and somewhat lower only on the bottom floor to be covered.
Multi-floor installations: Receivers **must** be mounted over one another in multi-floor installations. This helps maintain proper floor-to-floor reception.



Select a mounting location that:
– provides a clear line-of-sight of the protected area, if possible,

– is at least 30 m (1 ft) away from metal objects such as HVAC ducts,
– is on an inside wall, if possible,
– is 1.5 to 1.8 m (5 to 6 ft) from the floor,
– is not at a barrier where it is important to resolve which side an alarm location is on, and
– will not be damaged by tampering or opening doors.

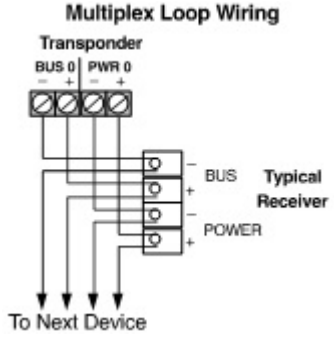
Outdoor receiver installation
Receiver spacing: Receivers should be mounted every 91.5 m (300 ft). It is very important to maintain as consistent spacing as possible, as this will ensure optimum signal locating. The more receivers that can detect a transmitted signal, the more accurate the locating will be. Each receiver should have a clear line-of-sight of the intended protection area.
Mounting height: Receivers should be mounted 3 m (10 ft) above grade. Maintain a mounting height that is as consistent as possible to ensure optimum signal locating.
Overhangs/eaves: Receiver locations should be below building overhangs and eaves. Most transmissions will occur a few feet (1 m) above grade; mounting above overhangs and eaves could result in inaccurate signal locating. Be especially careful around metal roofs as these can block the signal.

Select a mounting location that:
– provides a clear line-of-sight of the protected area,
– is away from metallic objects such as chain-link fences and electrical transformers. If coverage is required near such items, testing should be performed near these items to determine the potential need for additional receivers,
– is 3 m (10 ft) above grade,
– is not at a barrier where is it important to resolve which side an alarm location is on,
– is easy to service, and
– will not be damaged by tampering.

4.4.3 Wiring

Notice!
Apply power only after all connections have been made and inspected.

Connect wiring as shown:



4.4.4 Switches and jumpers

Loop address

The rotary switch is used to select the loop address. This is the address that is reported to the transponder which the receiver is connected to. Each device on a loop should have its own address. Only addresses 0 through 7 are valid. Do not use addresses 8 and 9.

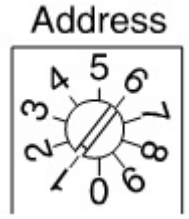


Figure 4.5: Address Switch

There are two groups of jumpers on the EA102A-304 Receiver. The first group contains jumpers P1 through P3. The second contains jumpers P4 through P8. The function of each jumper is indicated in the table below:

Jumper	Operation with Jumper in Place
P1*	Sounder is enabled
P2*	Green LED is enabled
P3*	Red LED is enabled
P4**	Test Mode is enabled
P5**	Receiver Spacing Mode is enabled
P6**	Left Antenna is disabled
P7**	Right Antenna is disabled
P8	Do not place a jumper across these pins.

Notice!

* Remove jumpers P1, P2, and P3 when installed in an outdoor enclosure.

** Remove jumpers P4, P5, P6, and P7 for normal operation.

Test mode

The module goes into test mode when jumper P4 is in place (jumper P5 removed). In this mode, all test and alarm receptions will be sounded.

Notice!

The sounder and LEDs (jumpers P1, P2, and P3) must also be enabled to operate the test mode.

Each receiver should be tested using the following method (test only one receiver at a time):

1. Enable the test mode by placing the jumper P4 across both pins (jumper P5 removed).
   – The red LED will turn ON and stay ON during the test.

- The green LED will flicker if the receiver is connected to a working transponder.
- There will be no data transmitted to the central station.
- The central station will receive a "not responding" failure.

2. Activate the transmitter from at least five different locations near the receiver.
   - The LEDs will respond to a received transmission.
   - If the receiver detected all the packets from the transmission, the sounder will beep three times.
   - If the receiver detected the transmission, but some of the packets were missing, it will beep once. This could indicate that the signal is not sufficient from this location.

Testing receiver spacing

Receiver spacing mode is enabled with jumper P5 in place (jumper P4 removed). This mode is exactly the same as the test mode above, except that only transmissions with an adequate receive margin are sounded. This indicates the maximum acceptable spacing of receivers. Use the following procedure to test the spacing of receivers:

1. Mount the first receiver.
2. Take the second receiver and a transmitter a distance away from the first receiver.
3. Activate the transmitter.
4. If receiver 1 sounds the test beeps, receiver 2 is within range. Repeat this test until receiver 1 no longer sounds the test beeps. Move back to the last location where receiver 1 received the test beeps. This location marks the maximum spacing between receivers. Mount receiver 2 at this location or closer to receiver 1.

Notice!

Do not use the test mode (jumper P4) to determine receiver spacing.

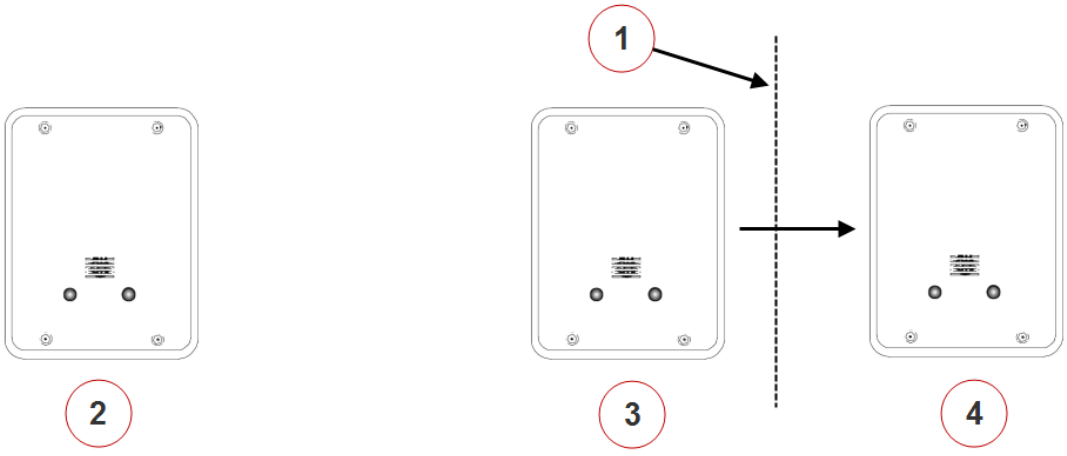
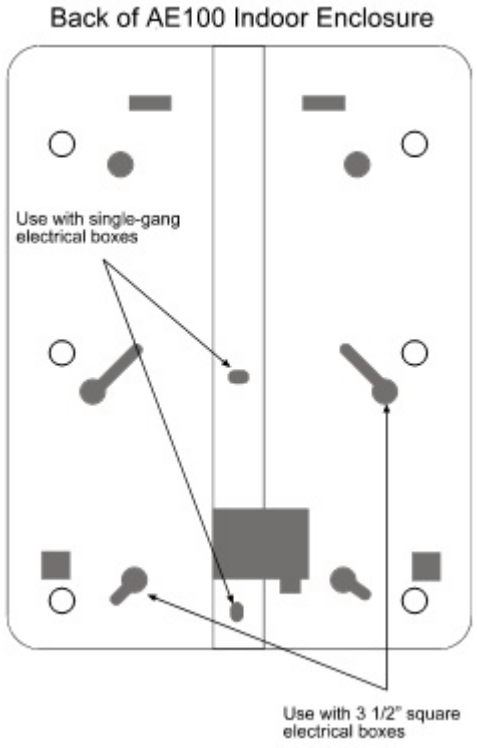


Figure 4.6: Receiver Spacing

1	Receiver 1 stops sounding the test beeps when receiver 2 is moved past this point	3	Receiver 2 at maximum range
2	Receiver 1	4	Receiver 2 beyond maximum range

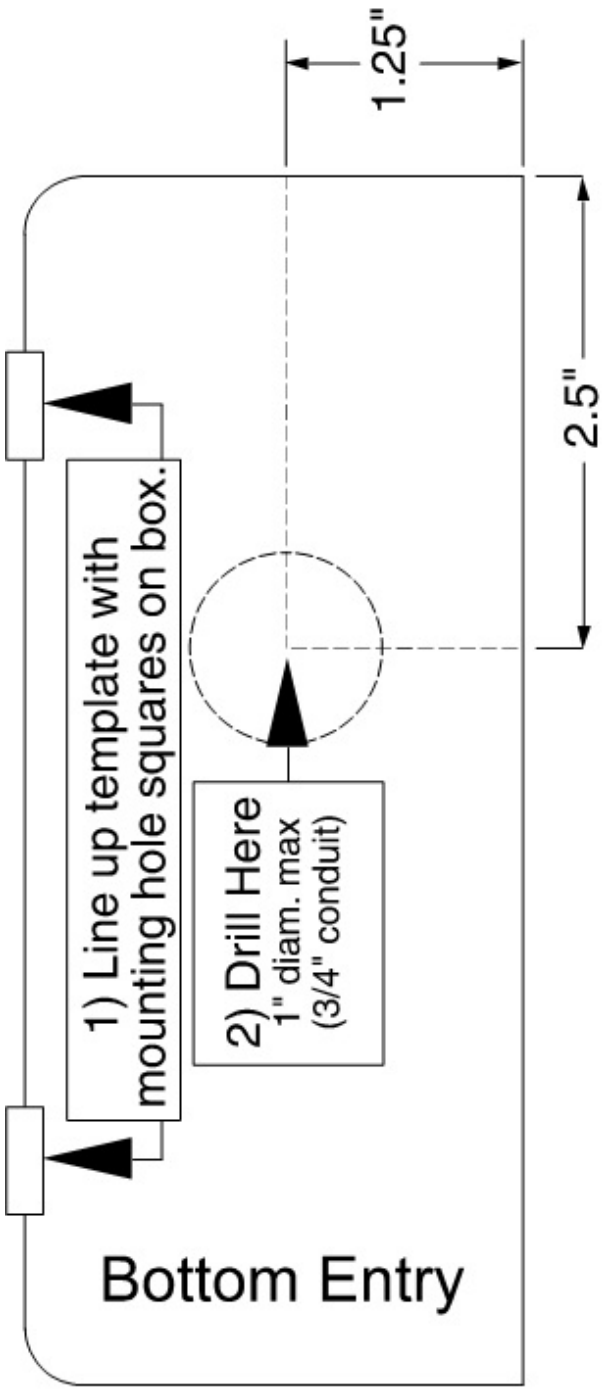
4.4.5 Pre-wired installations

When mounting the enclosure to a pre-wired electrical box, make sure that the electrical box has a six inch overhead clearance. The enclosure should be mounted as shown below:



4.4.6 Drilling templates

Use the following templates for mounting the AE101 outdoor enclosure. Remember to remove jumpers P1, P2, and P3 prior to installing the receiver.


1.25"
2.5"
1) Line up template with mounting hole squares on box.
2) Drill Here
1" diam. max
(3/4" conduit)
Bottom Entry

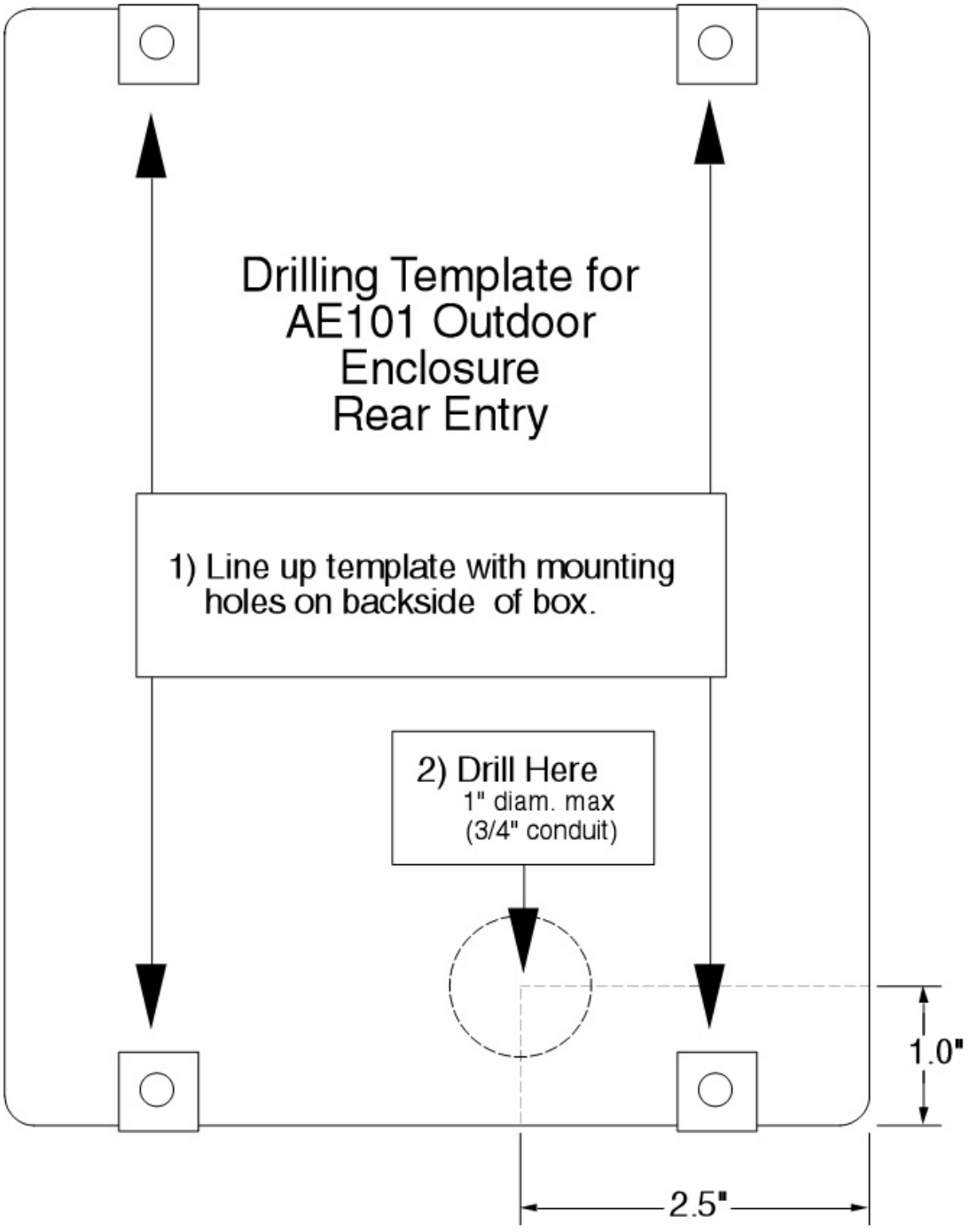


Figure 4.7: Drilling Template for AE101 Outdoor Enclosure Bottom Entry

4.5 EA120B alert unit

4.5.1 Specifications

Electronics: EA120B

Enclosures: *Indoor*: AE1 (9"H x 7"W x 1.75"D)
Outdoor: AE101 (14.75"H x 12.75"W x 3.5" D)

Hardware Kits:	*Indoor*: H500	
	Outdoor: H121	
	Temperature Range	-40 °F to + 149 °F (-40 °C to +65 °C)
	Power	18 V AC, 50 VA
	Battery Backup	12 V DC Lead Acid Battery
Accessory Equipment	Horn/Strobe: E28000B • Strobe: 500 mA solid state sink, terminal switches to ground in an alarm condition. • Siren: 500 mA solid state sink, terminal switches to ground in an alarm condition. • Power: 12 V @ 1A, max.	
	Transformer:	TR1850
	Batteries (3 Amp Hour):	E28629B
	(7 Amp Hour):	E19729B
	Battery Cables:	C316 (3 or 7 Amp) C315 (17 Amp) C311 (3 or 7 Amp expansion)
Compatibility	EA500B ROM Version 4.00 or higher	

4.5.2 General information

The alert unit is a driver for output modules such as Security Escort's E28000B horn/strobe. The unit should be mounted indoors; however, an outdoor enclosure is available. The horn/strobe should always be mounted outdoors.

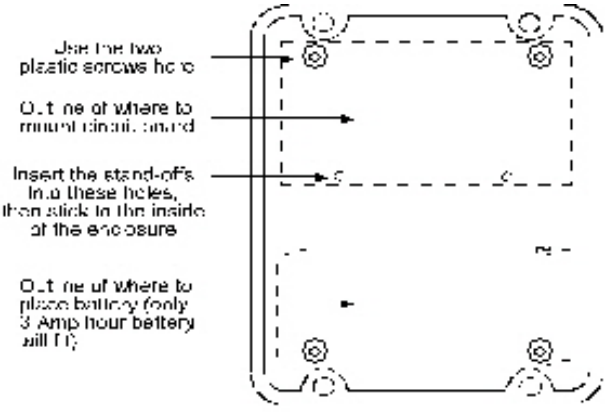
The alert unit gets its main power (for horn/strobe activation) from the 18 V AC transformer and its backup power from a battery; however, the multiplex bus will continue to supply the transponder information on status and troubles in the event "local" power is lost.

4.5.3 Mounting

Normally, the enclosures are mounted first and all the wiring run, then the electronics are mounted, wired, and tested.

The enclosures come with their own mounting hardware. The hardware kits listed above are for mounting the circuit board to the enclosures (the indoor hardware kit also includes a tamper switch and a lock and key).

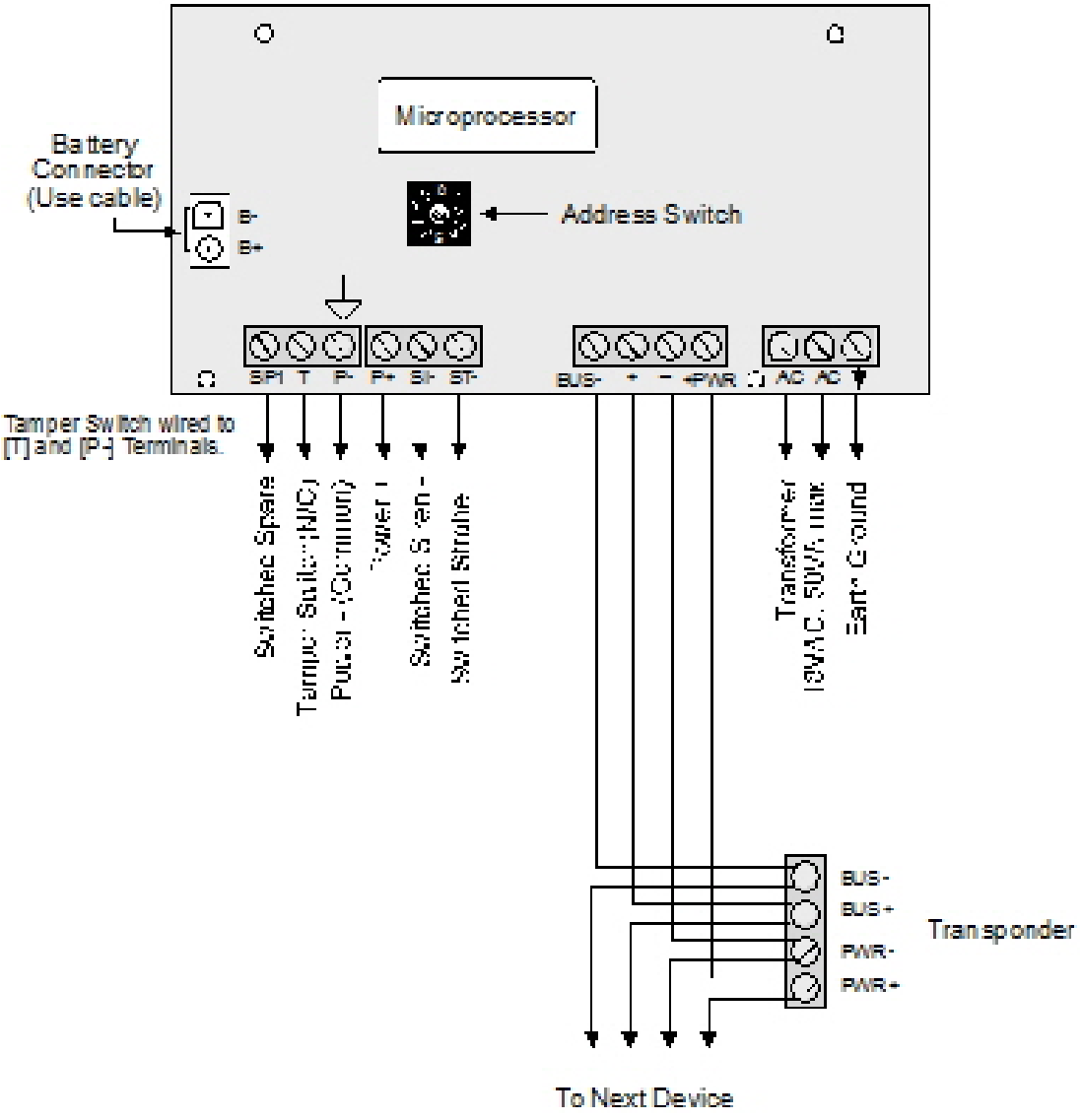
Mount the circuit board to the enclosure as indicated in the figures below.



Inside of AE101 Enclosure

4.5.4 Wiring

Wire the alert unit using the figure below:



4.5.5 Set the address

Every module on each multiplex bus of the transponder must have its own address. Set the address on the alert unit using the address switch.

Use only address numbers 0 through 7. **Do NOT use address numbers 8 and 9**.

4.6 Moxa interface

4.6.1 Introduction

The Moxa interface is used between the RS-232 signal bus of the Security Escort transponder, and the Ethernet connection of the Local Area Network (LAN) in order to communicate with the Security Escort Central Console.

4.6.2 Specifications

Recommended Model:	NPort 5150
Dimensions:	52 mm (2.05 in) x 80 mm (3.15 in) x 22 mm (0.89 in)
Power:	Use the included 12 – 48 V DC on barrel connector
Recommended Cable:	Standard male DB9 to female DB9 serial cable (not included).

4.6.3 Installation and operation notes

- The Moxa device must be powered at all times. Use the included power adapter.
- A standard male DB9 to female DB9 serial cable is used to connect the transponder to the Moxa device.
- Instructions on setting up the Moxa device is based on the recommended model NPort 5150 (firmware version: 3.4 Build 11080114).

The pinouts of male DB9 serial port of Moxa NPort 5150 are as follows:

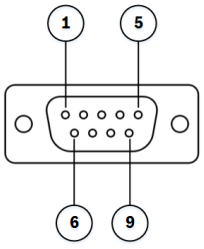


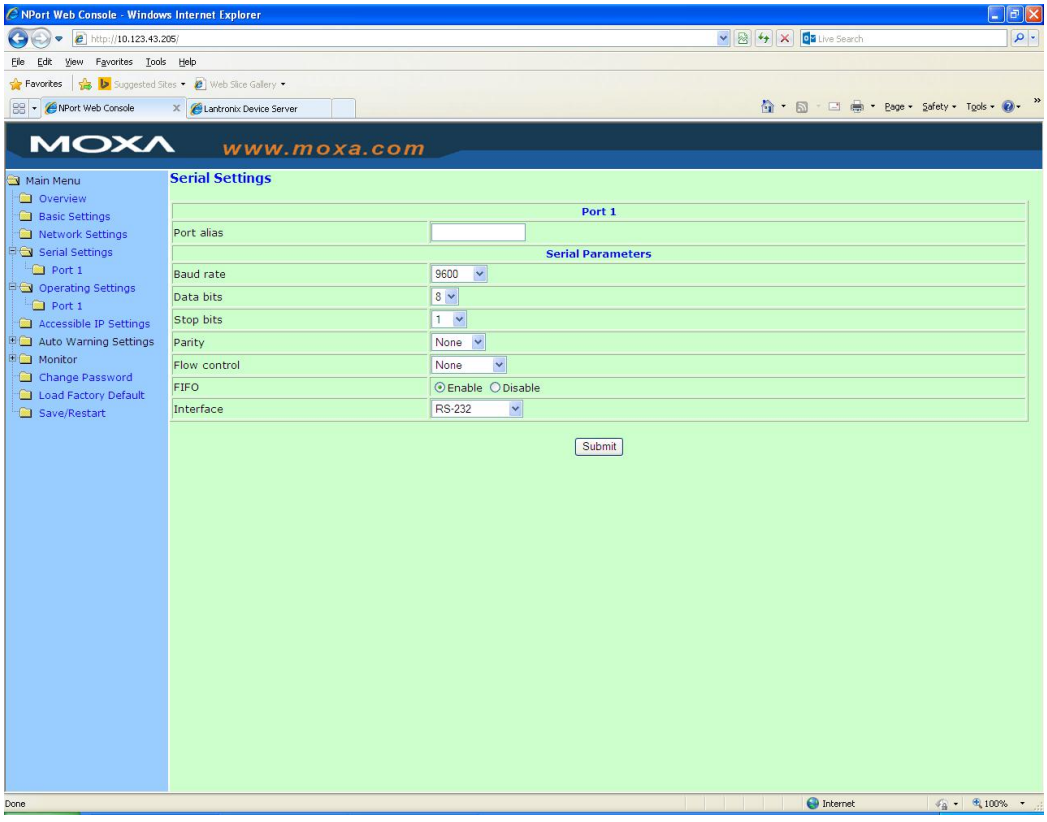
Figure 4.8: Moxa NPort 5150 Male DB9

Pin Number	RS-232	RS-422/RS-485 (4W)	RS-485 (2W)
1	DCD	TXD-(A)	--
2	RxD	TXD+(B)	--
3	TxD	RXD+(B)	Data+(B)
4	DTR	RXD-(A)	Data-(A)
5	GND	GND	GND
6	DSR	--	--
7	RTS	--	--
8	CTS	--	--
9	--	--	--

Notice!
Third party user interfaces are subject to change without notice at the sole discretion of the respective providers but configuration setting shall remains as specified.

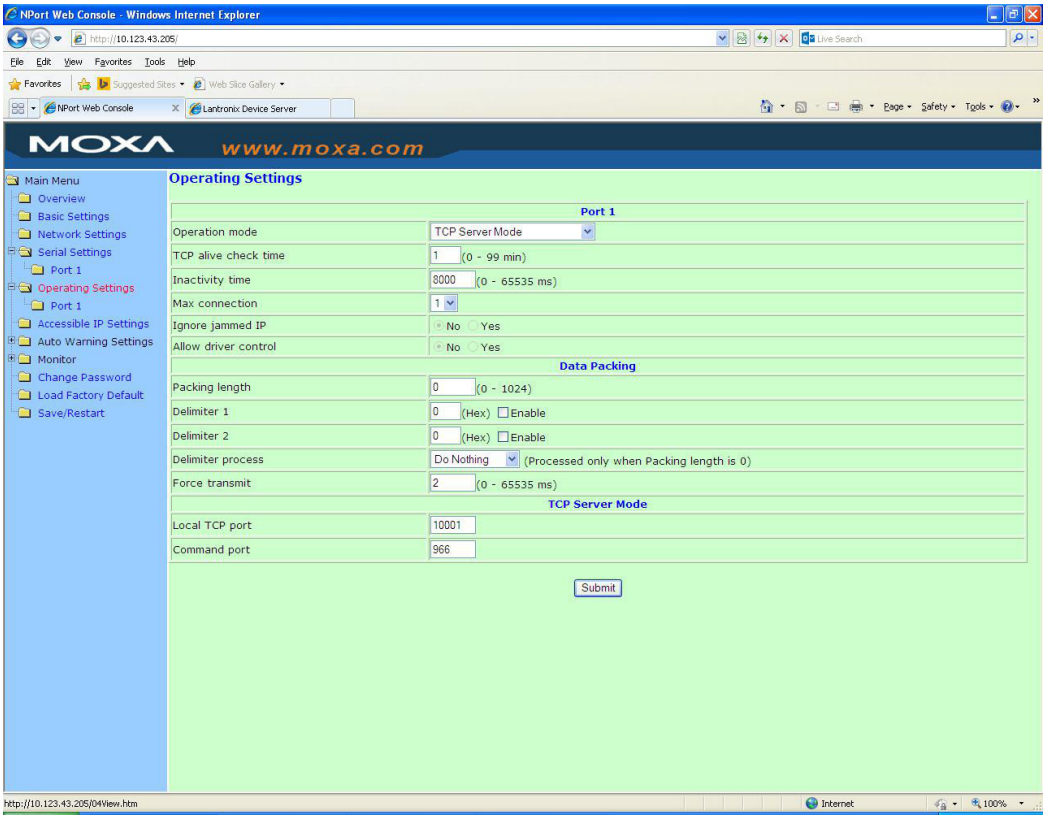
Follow the instructions below to set up the NPort 5150 device and use the serial cable to connect the transponder to the Ethernet network.

1. Connect NPort 5150 to the Ethernet network.
2. Set up and configure the IP address of the Moxa device. There are several methods to configure the IP address. Please refer to the *Moxa User Manual* on steps to configure the IP address.
3. From a computer on the Ethernet network, login to the Moxa device using the web browser interface.
4. Go to **Serial Settings** > **Port 1**. Remove any entry in the **Port alias** field (it must be empty). Set the **Baud Rate** field as “9600”, the **Data Bits** field as “8”, the **Stop Bits** field as “1”, the **Parity** field as “None”, the **Flow Control** field as “None”, the **FIFO** field as “Enable” and the **Interface** field as “RS-232”.



5. Click the **[Submit]** button to make the changes and restart the Moxa device.
6. Go to **Operating Settings** > **Port 1**. It is recommended to enter “1” in the **TCP alive check time** field, “8000” in the **Inactivity time** field, and “2” in the **Force transmit** field. Please refer to the *Moxa User Manual* for further details. Enter the port number of the transponder in the **Local TCP Port** field. This port number must be the same number as

the one that is set for the transponder in the **Transponder Database** of the Security Escort software.



7. Click the **[Submit]** button to make the changes and restart the Moxa device.
8. The connecting cable is a male DB9 to female DB9 serial cable. Connect the male DB9 connector to the transponder and the female DB9 connector to the Moxa device.

4.7 Lantronix interface

4.7.1 Introduction

The Lantronix interface is used between the RS-232 signal bus of the Security Escort transponder, and the Ethernet connection of the Local Area Network (LAN) in order to communicate with the Security Escort Central Console.

4.7.2 Specifications

Recommended Model:	UDS1100
Dimensions:	90 mm (3.5 in) x 64 mm (2.5 in) x 23 mm (0.9 in)
Power:	Use the included 9 – 30 V DC on barrel connector
Recommended Cable:	Modified male DB25 to male DB9 serial cable (do not use the serial cable included)

4.7.3 Installation and operation notes

– The Lantronix device must be powered at all times. Use the included power adapter.

– Do not use the female DB9-to-male DB25 serial cable included. A modified serial cable must be used to connect the transponder to the Lantronix device.
– Instructions on setting up the Lantronix device is based on the recommended model UDS1100.

The pinouts of female DB25 serial port of Lantronix are as follows:

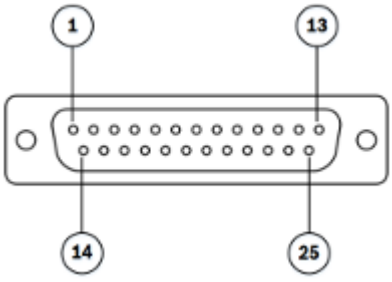


Figure 4.9: Lantronix UDS1100 Female DB25

Pin Number	RS-232 Signals
1	Chassis Ground
2	Transmit Data
3	Receive Data
4	Request to Send
5	Clear to Send
6	Data Set Ready
7	Signal Ground
8	Carrier Detect
9	---
10	---
11	Receive Clock Out
12	---
13	---
14	---
15	Transmit Clock In
16	---
17	Receive Clock In
18	Local Loopback
19	---
20	Data Terminal Ready
21	Remote Loopback

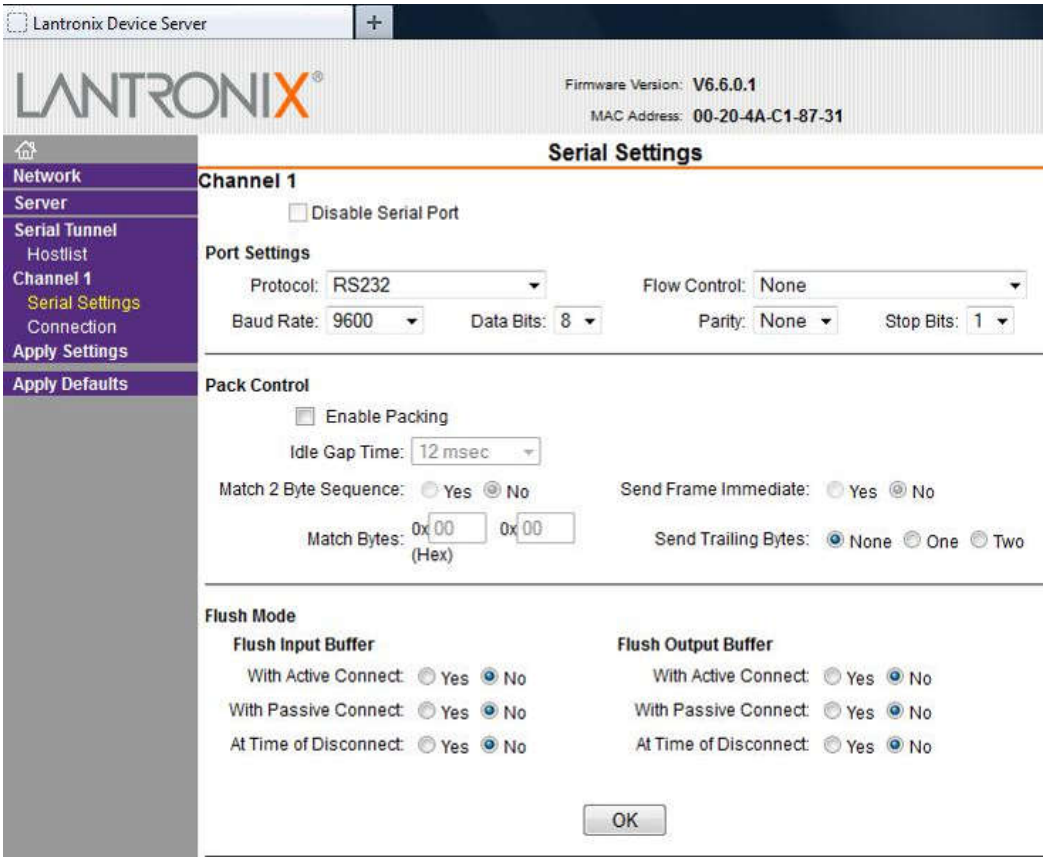
Pin Number	RS-232 Signals
22	---
23	---
24	Transmit Clock Out
25	Test Mode

Notice!

Third party user interfaces are subject to change without notice at the sole discretion of the respective providers but configuration setting shall remains as specified.

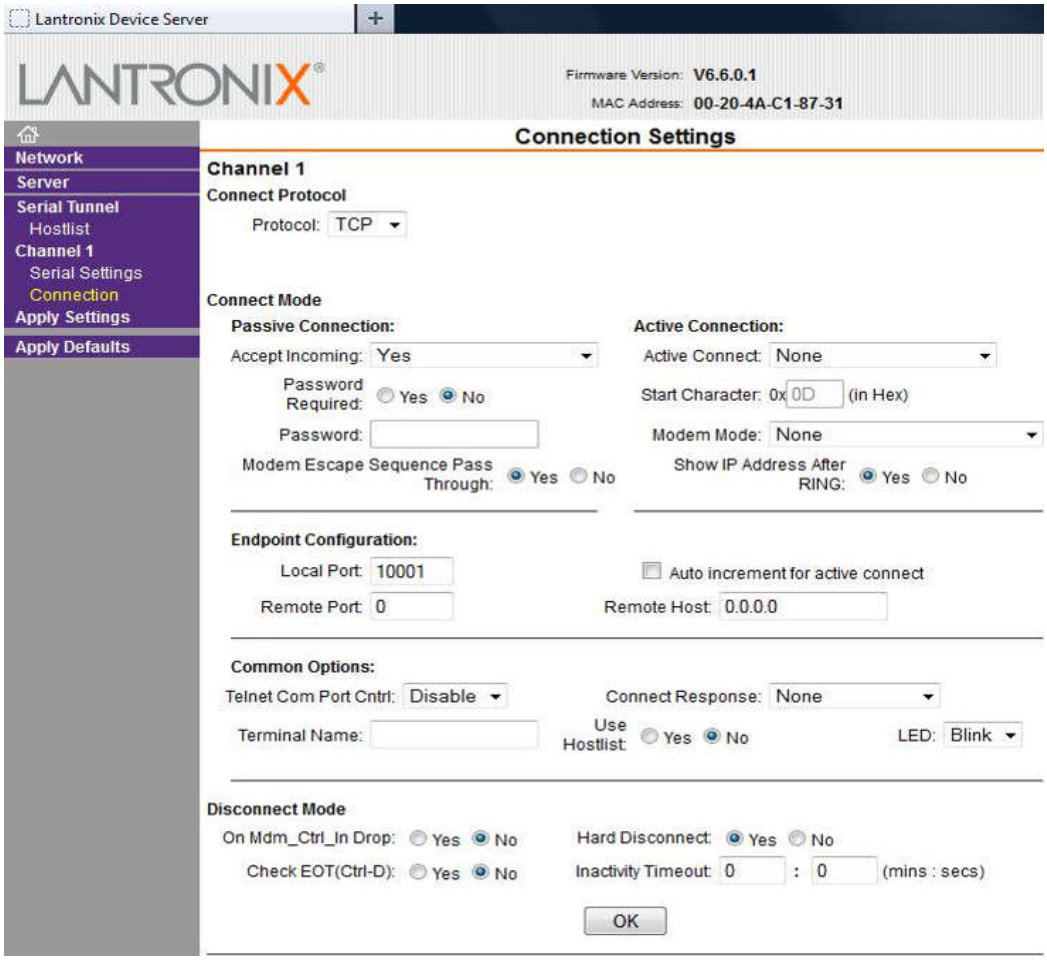
Follow the instructions below to set up the UDS1100 device and modify the serial cable to connect the transponder to the Ethernet network.

1. Connect UDS1100 to the Ethernet network.
2. Set up and configure the IP address of the Lantronix device. There are several methods to configure the IP address. Refer to the Lantronix User Guides on steps to configure the IP address.
   Connect the Lantronix device to the Ethernet network.
3. From a computer on the Ethernet network, login to the Lantronix device using the web browser interface with the default user ID and password.
4. Go to **Channel 1** > **Serial Settings**. Configure the **Protocol** field as “RS232”, the **Flow Control** field as “None”, the **Baud Rate** field as “9600”, the **Data Bits** field as “8”, the **Parity** field as “None”, and the **Stop Bits** field as “1”.



5. Click the **[OK]** button to apply the settings,

6. Go to **Channel 1** > **Connection**. Select “TCP” from the drop down list of **Protocol** field. Enter the port number of the transponder in the **Local Port** field. This port number is the same number as the one that is set for the transponder in the **Transponder Database** of the Security Escort software.



7. Click the **[OK]** button to apply the settings.
8. The connecting cable is a modified male DB9 to male DB25 serial cable. Only 3 wires are compulsory for the modification of DB9 to DB25 cable as illustrated in the table below.

RS232 Pin Assignment	
DB9 Pin Male	**DB25 Pin Male**
Pin	**Pin**
2	**2**
3	**3**
5	**7**

Table 4.3: Wiring – Required pins

9. Connect the male DB9 connector to the transponder and the male DB25 connector to the Lantronix device.

4.8 SE485 interface

4.8.1 Introduction

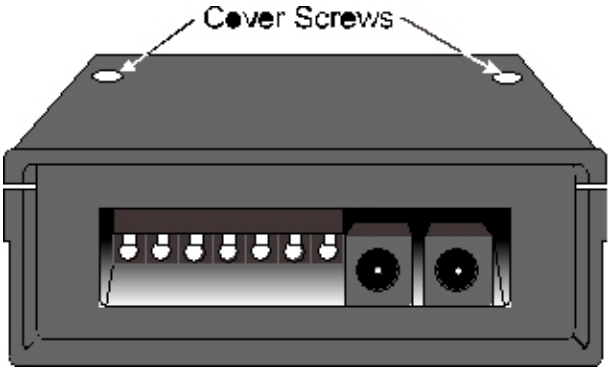
The SE485 is designed as an interface between the RS-485 signal bus of the Security Escort transponder, and the serial bus (RS-232) of the Security Escort Central Console.

4.8.2 Specifications

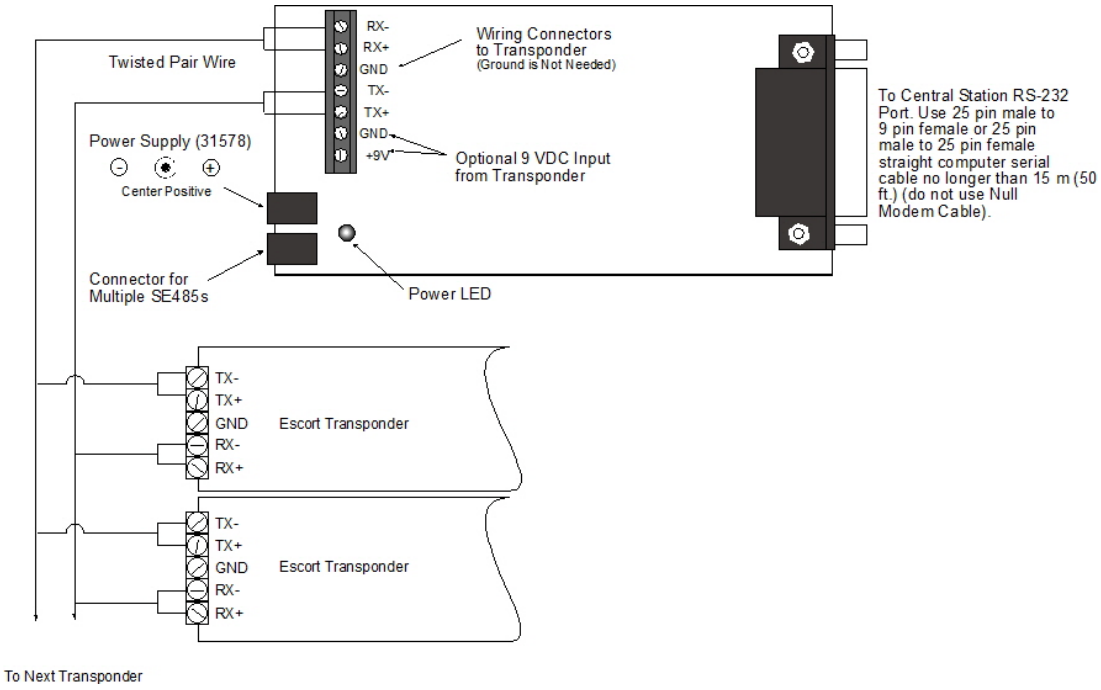
Dimensions:	135 mm (5.375 in) x 85 mm (3.031 in) x 30 mm (1.187 in)
Power:	Use the included 120 V AC adaptor to 9 V DC, 300 mA or power from the transponder
Recommended Cable:	2 twisted pair, 4 conductor, 22 AWG (0.8 mm)
Compatibility	EA500B transponder EA501B transponder

4.8.3 Installation and operation notes

– Remove the cover by removing the cover screws shown below.



– Connect the wiring as shown below.

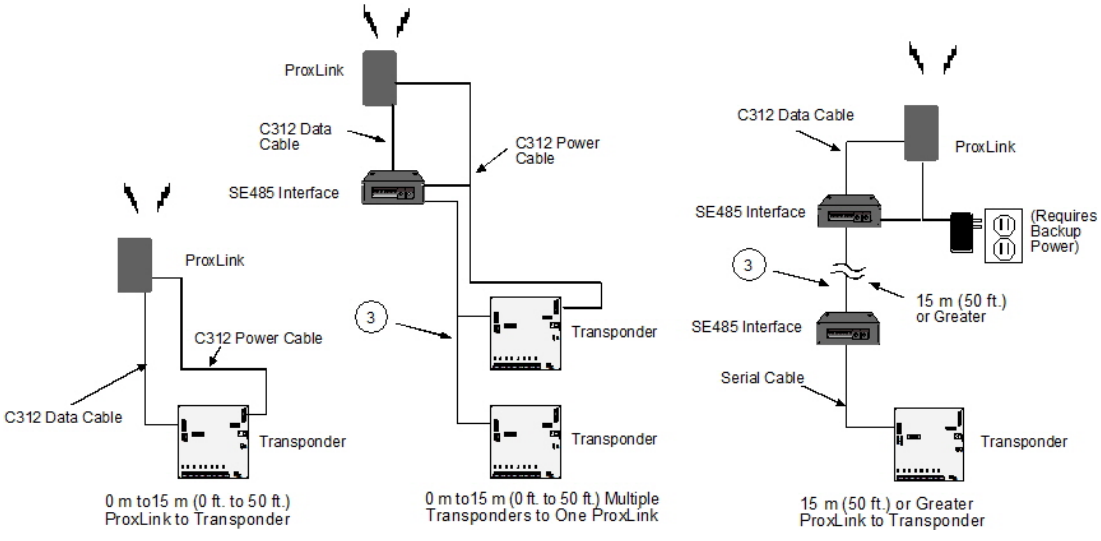


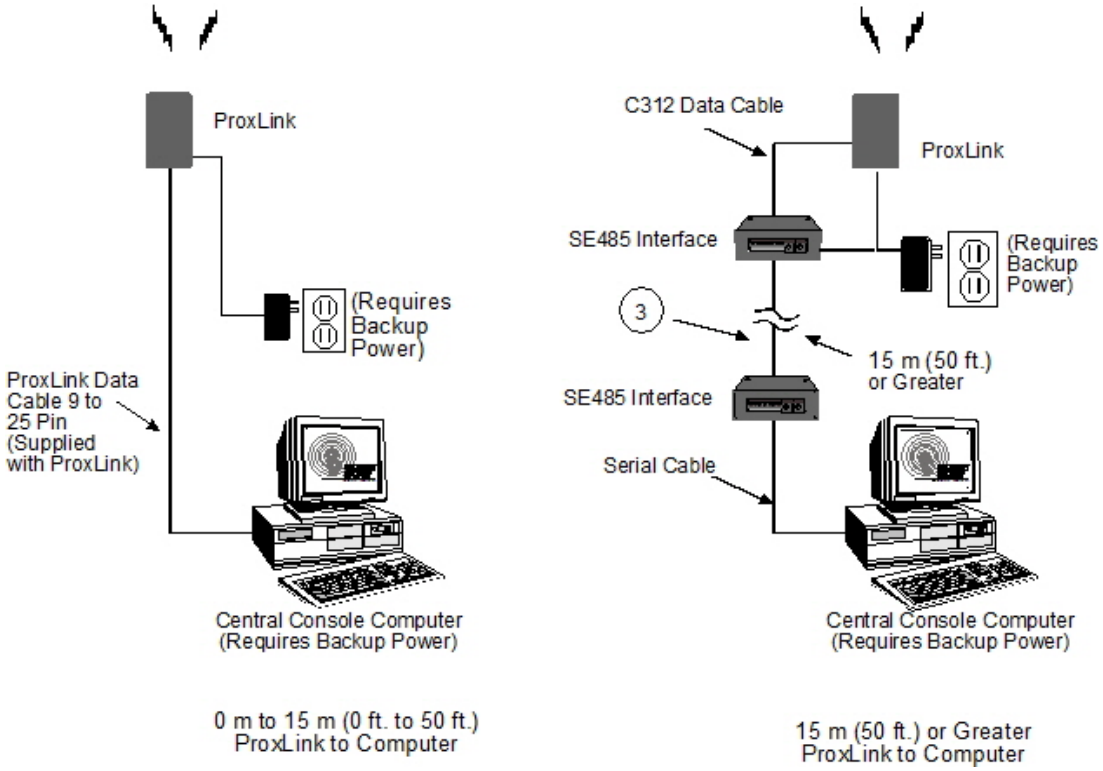
– After wiring the system, replace the cover and power up the unit.

Operation notes

– Each transponder must have its own address.
– For the Security Escort ® system to maintain operation, the SE485 must be powered at all times. Use the 9 V adaptor provided plugged into an uninterrupted power supply (UPS).
– The SE485 may also be powered from the transponder's 9 V output connected to the 9 V DC input wiring connectors.
– Up to four SE485s can be included in an installation. If using multiple SE485s, use the connector cable provided.

4.9 ProxLink setup




ProxLink
(Requires Backup Power)
ProxLink Data Cable 9 to 25 Pin (Supplied with ProxLink)
Central Console Computer (Requires Backup Power)
0 m to 15 m (0 ft. to 50 ft.) ProxLink to Computer
C312 Data Cable
ProxLink
SE485 Interface
(Requires Backup Power)
3
15 m (50 ft.) or Greater
SE485 Interface
Serial Cable
Central Console Computer (Requires Backup Power)
15 m (50 ft.) or Greater ProxLink to Computer

Configuration procedure

Notice!

For more details refer to the *ProxLink Radio Module User's Manual*

Required equipment

- ProxLink Radio Module
- PC with RS-232 port running a terminal emulation software package. Select **Start > Programs > Accessories > Hyper Terminal**.
- ProxLink DB-9 to DB-25 Female RS-232 Cable
- 9 V DC Power Supply

Configure

Select one of seven radio channels (902 MHz to 928 MHz). Make certain that the channel chosen is the same for all the ProxLink located at the transponders and for the ProxLink at the Central Console computer.

Select one ProxLink for your Central Console computer. The serial number (located on a silver tag on the bottom of the ProxLink) of this ProxLink must be entered in the **Destination Serial Number** and **Serial # Filter** location on all ProxLink Radios connected to the transponders.

1. Attach the PC to the ProxLink using the ProxLink RS-232 cable. Attach the DB-9 Connector to the ProxLink and attach the DB-25 female connector the PC. Gender changers or DB-25 to DB-9 converters may be required depending on your serial port connector type.
2. Start your terminal emulation software (Hyper Terminal). Configure the ProxLink as follows: 9600 Baud, 8 Data Bits, 1 Stop Bit, and no parity.

3. Put the ProxLink in User Interface Mode by pressing the **[CONFIGURATION]** button on the front of the unit. The ProxLink should respond by displaying the **Main Menu** screen.
4. Once the **Main Menu** is displayed, configure a ProxLink parameter by selecting a menu option and pressing the <Enter> key. This will either display a prompt or a sub-menu. After finishing with a sub-menu, press the <Esc> key to return to the previous menu.
5. After you have finished configuring the ProxLink, type <L> <Enter>, then type <Y> to place the unit in operating mode.

Configuration should look as follows in Main Menu, D - Display ProxLink Radio Module Parameters:

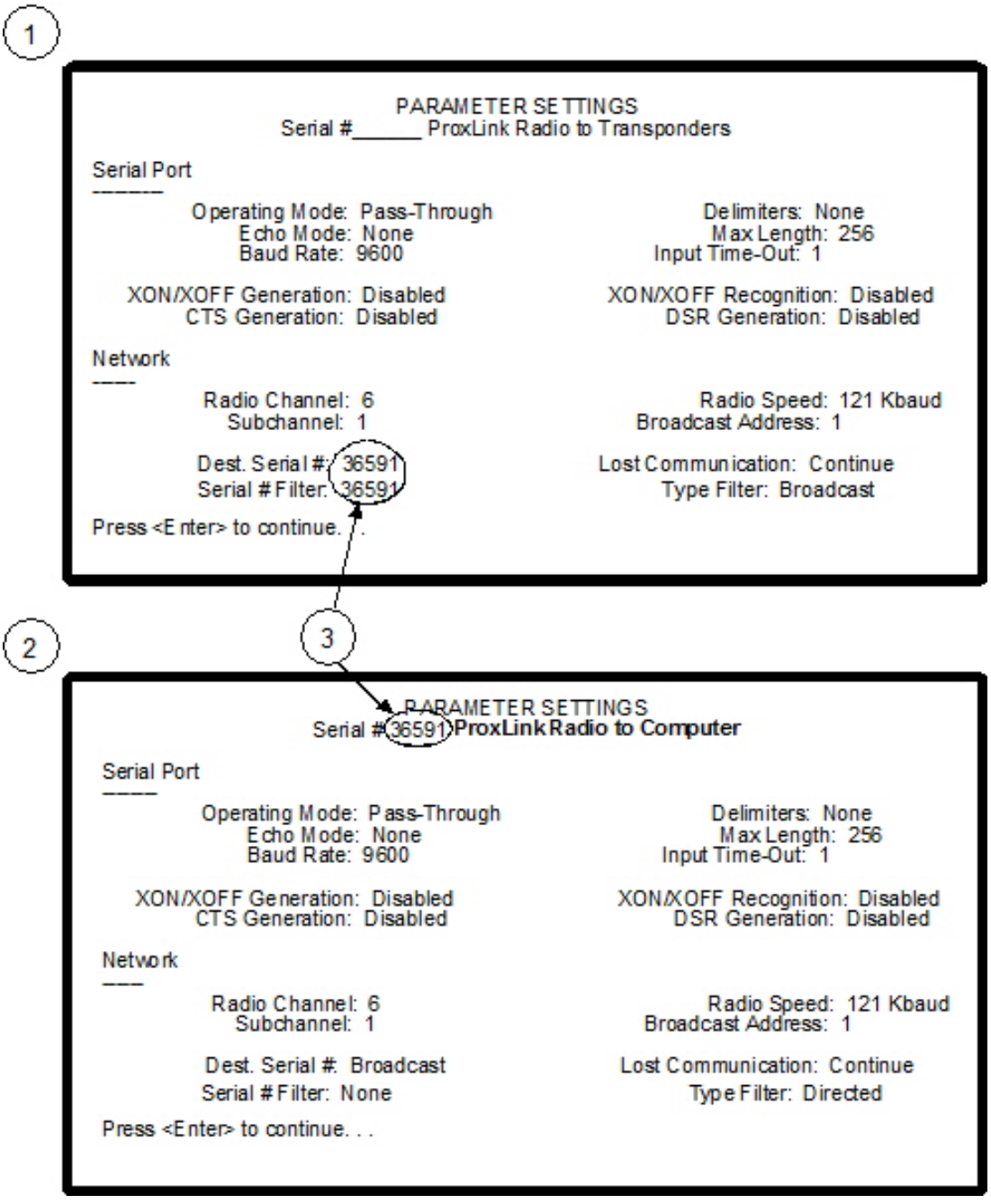


Figure 4.10: ProxLink Radio Module Configuration

1	ProxLink radio module configuration for the transponders	3	These numbers must match
2	ProxLink radio module configuration for the central station		

5 Installation options

5.1 Demo installations

When the software is used for demo purposes, it is limited to ten records in the **Subscriber Database**, one transponder in the **Transponder Database** and only receivers 0 through 3 on bus 0 can be defined for that transponder (no other points can be programmed for that transponder). If these limitations are observed, the software will communicate with the single transponder and the system can be used with full functionality for demo purposes. Refer to the Installing the Security Escort software section of to install the software.
After the software has been installed, do not run it. Double-click the HDD32.EXE file in the Security Escort directory (“C:\ESCORT”). This will install the driver for the software key. This is required even for demo installations that will not have the software key. If the HDD32.EXE installer is not run before the Security Escort software is run the first time, the Security Escort software will stop with an error and HDD32.EXE will automatically run. The demo installation is complete at this point and you do not have to refer to the rest of this document.
In demo mode, communications are allowed to one transponder even if the **Transponder Database** has more than one transponder in it for diagnostic purposes. The transponder selected in the **Transponder current status** or **Transponder communications** dialog will be the transponder that can be communicated with. The transponder can be reselected at any time to change the current transponder in communication. All tests, supervisions and maintenance alarms will function normally; however only subscriber alarms that contain reports from receivers 0 through 3 on bus 0 will function. If an alarm also includes other receivers reporting, that alarm will be ignored. Therefore, actual Security Escort operation can be demonstrated using up to 4 receivers. Also a demo system can be used to directly connect to transponders using the actual transponder database from the system to perform all functions except subscriber alarms. This is desirable to allow a laptop to be plugged directly into a transponder to diagnose problems. In both of these modes the **Subscriber Database** must have five or less subscribers.

5.2 Non-Network installations

If this system is not using the network to connect master, slave and workstation computers, refer to the Security Escort software installation section of this document to install the software. After the software has been installed, do not run it. Plug the software key into the USB port on the computer and double-click the HDD32.EXE file in the Security Escort directory (“C:\ESCORT”). This will install the driver for the software key.
If the HDD32.EXE installer is not run before the Security Escort software is run the first time, the Security Escort software will stop with an error and HDD32.EXE will automatically run. A non-network installation is complete at this point and you do not have to refer to the rest of this document.

5.3 Network installations

The Security Escort software supports a single master computer, a single slave computer (optional) and a maximum of eight workstations (limited to the number programmed in the software key). The master computer normally processes the real time communications to the transponders and controls the system. The slave computer can assume the master’s role by switching the transponder communications to the slave computer. This system redundancy feature is explained in further details in *System redundancy, page 172*. The workstation computers allow other computers to respond to alarms, perform maintenance and edit the databases.

5.4 Installing the Security Escort software

5.4.1 Software installation procedure

Typically the Security Escort program is delivered on a CD-ROM.

Notice!

Exit all other programs before inserting the CD-ROM.

An autorun feature should automatically start the installation program. If not, run SETUP.EXE using one of the following methods:

1. Double click the **Computer** icon on the desktop. Select the Compact Disc (X:), double-click the INSTALL directory. Double-click the SETUP.EXE icon. X is the letter of the CD-ROM drive.
2. Go to **Start** > **Programs** > **Windows Explorer**. In Windows Explorer, select the Compact Disc (X:) and double-click the INSTALL directory. Double-click the SETUP.EXE icon.
3. Click **Start** > **Run.** Type “X:\INSTALL\SETUP.EXE” in the **Open** textbox and click the **[OK]** button. X is the drive letter for the CD-ROM drive.

Once SETUP.EXE is running, the following **Welcome** dialog appears.

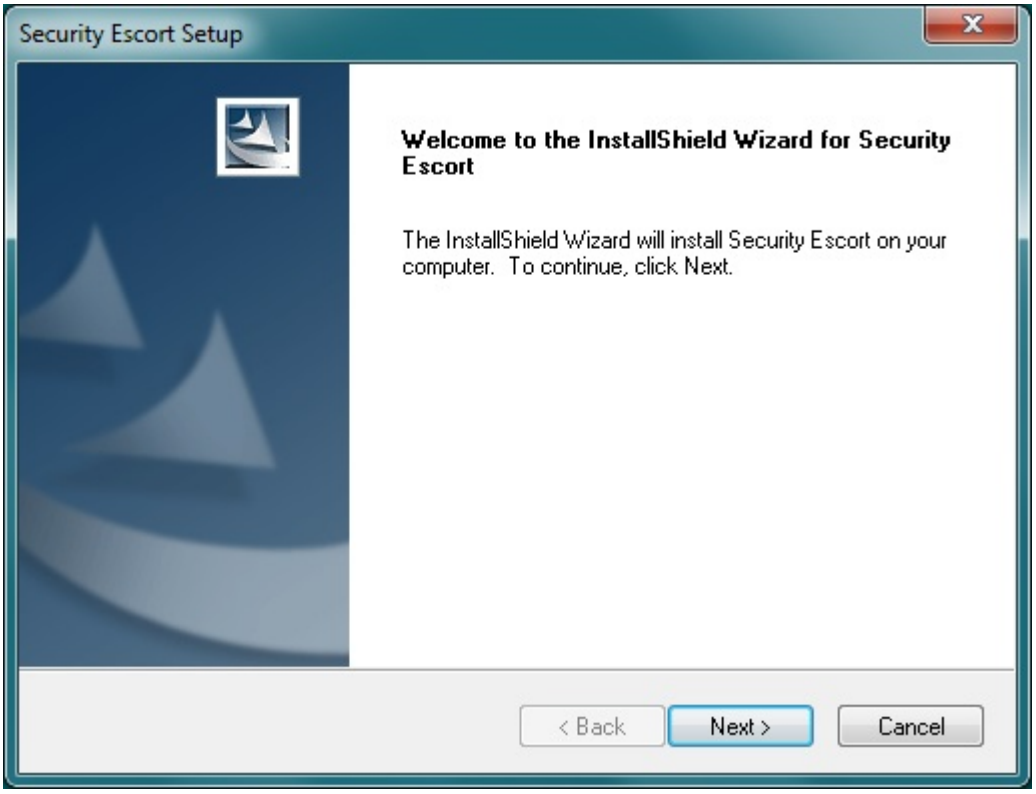

Security Escort Setup
Welcome to the InstallShield Wizard for Security Escort
The InstallShield Wizard will install Security Escort on your computer. To continue, click Next.
< Back
Next >
Cancel

Figure 5.1: Security Escort Setup Welcome Dialog

You can click the **[Cancel]** button at any stage of installation to abort installation. The **Exit Setup** dialog will appear. Click the **[Yes]** button to abort installation.

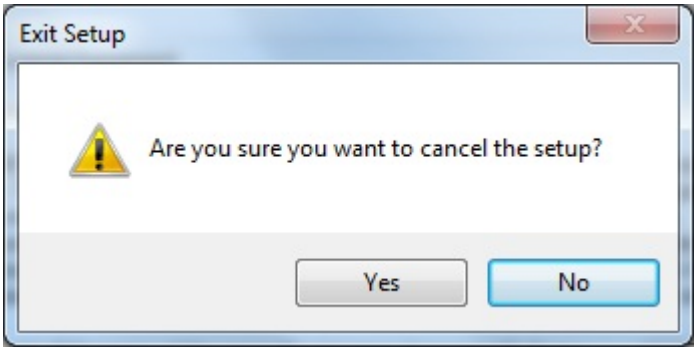


Figure 5.2: Exit Setup Dialog

Otherwise, click the **[Next >]** button. The **License Agreement** dialog appears.

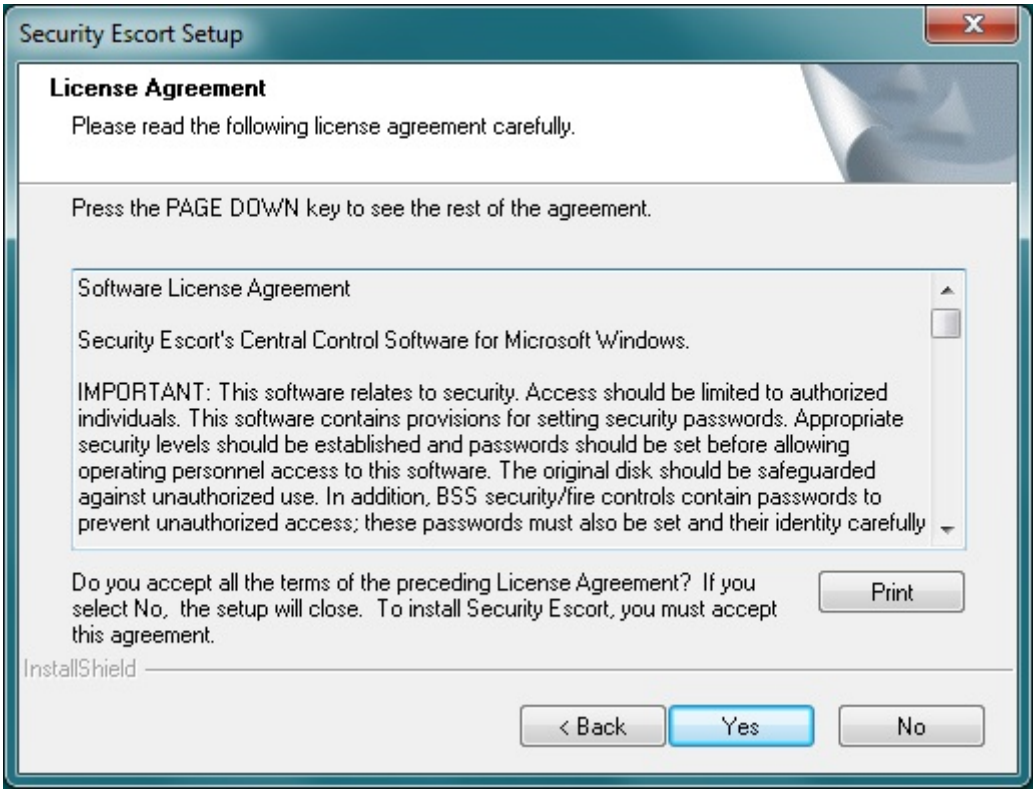

Security Escort Setup
License Agreement
Please read the following license agreement carefully.
Press the PAGE DOWN key to see the rest of the agreement.
Software License Agreement
Security Escort's Central Control Software for Microsoft Windows.
IMPORTANT: This software relates to security. Access should be limited to authorized individuals. This software contains provisions for setting security passwords. Appropriate security levels should be established and passwords should be set before allowing operating personnel access to this software. The original disk should be safeguarded against unauthorized use. In addition, BSS security/fire controls contain passwords to prevent unauthorized access; these passwords must also be set and their identity carefully
Do you accept all the terms of the preceding License Agreement? If you select No, the setup will close. To install Security Escort, you must accept this agreement.
Print
InstallShield
< Back
Yes
No

Figure 5.3: License Agreement Dialog

Click the **[Yes]** button to accept the License Agreement. The **Readme Information** dialog appears.

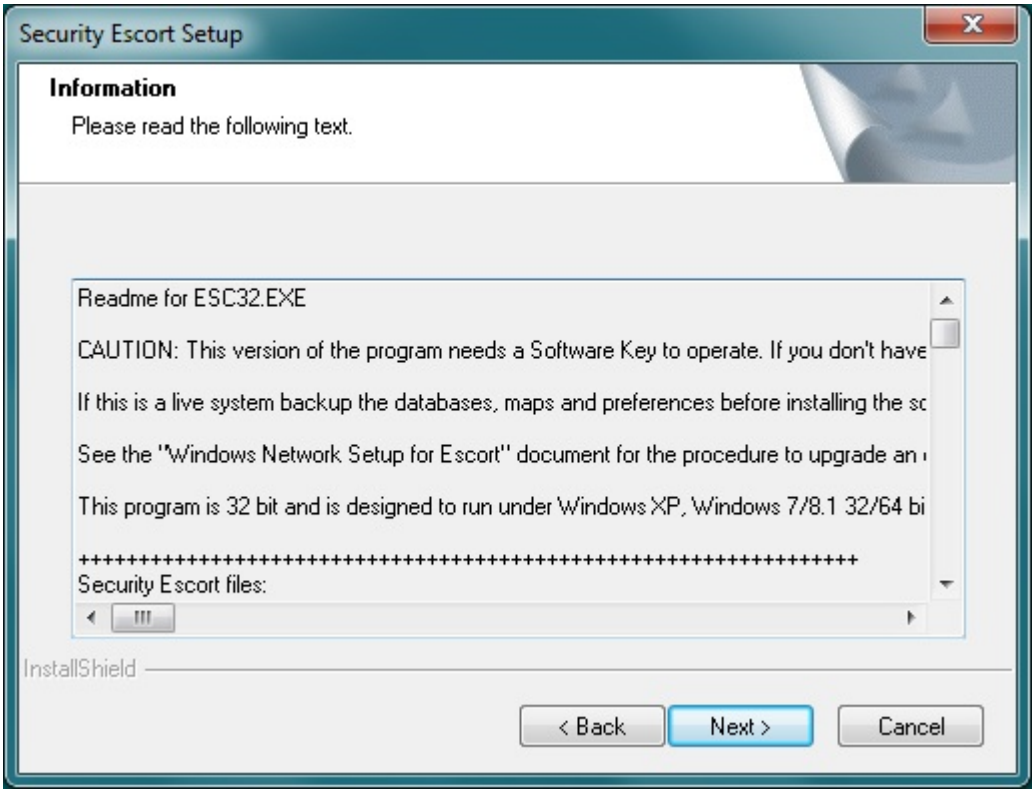

Security Escort Setup
Information
Please read the following text.
Readme for ESC32.EXE
CAUTION: This version of the program needs a Software Key to operate. If you don't have
If this is a live system backup the databases, maps and preferences before installing the sc
See the "Windows Network Setup for Escort" document for the procedure to upgrade an
This program is 32 bit and is designed to run under Windows XP, Windows 7/8.1 32/64 bi
++
Security Escort files:
InstallShield
< Back
Next >
Cancel

Figure 5.4: Readme Information Dialog

Read the entire file before proceeding (use the scroll bar on the right side to see the portion not currently displayed). Once done, click the **[Next >]** button. The **Choose Destination Location** dialog appears. Select the location on the hard disk drive to install the Security Escort program. Typically, the default location would be ideal (“C:\ESCORT”).

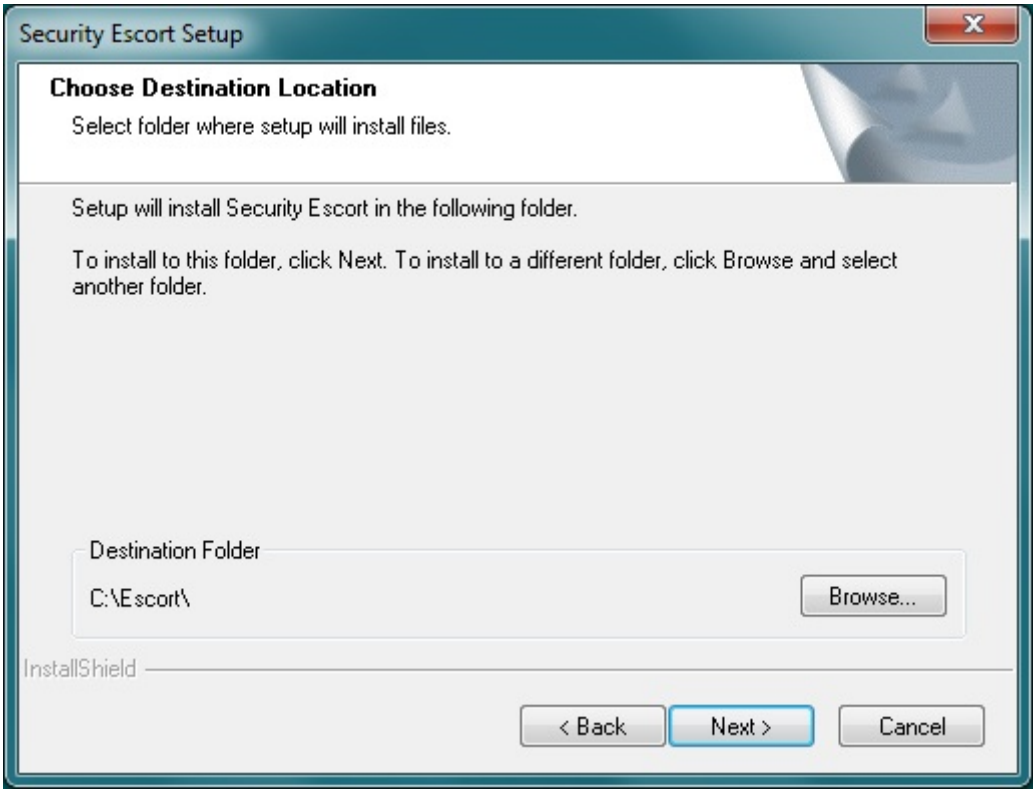

Security Escort Setup
Choose Destination Location
Select folder where setup will install files.
Setup will install Security Escort in the following folder.
To install to this folder, click Next. To install to a different folder, click Browse and select another folder.
Destination Folder
C:\Escort\
Browse...
InstallShield
< Back
Next >
Cancel

Figure 5.5: Choose Destination Location Dialog

If you wishes to install the program in a different location, click the **[Browse]** button and the **Choose Folder** dialog to appears. Select the desired folder and click the **[OK]** button. You will return to the **Choose Destination Folder** dialog.

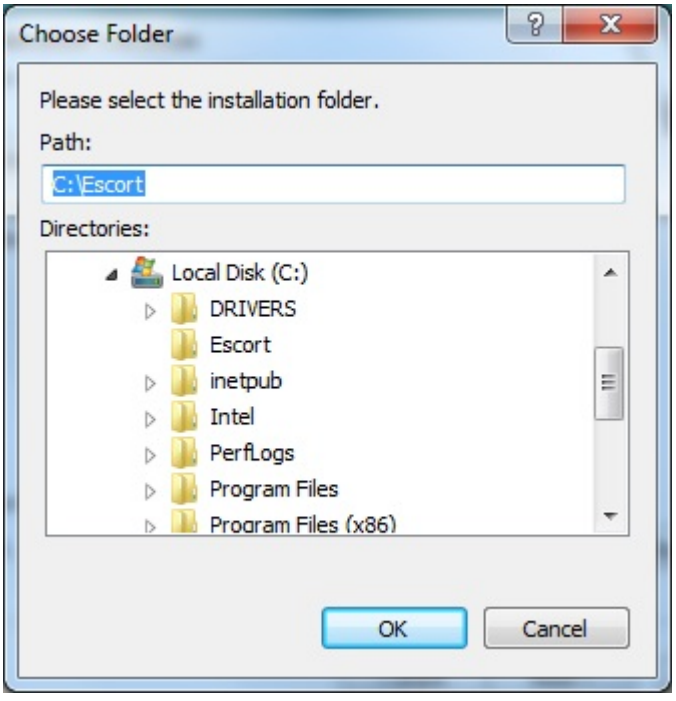


Figure 5.6: Choose Folder Dialog

Click the **[Next >]** button on the **Choose Destination Folder** dialog. The **Setup Type** dialog appears.

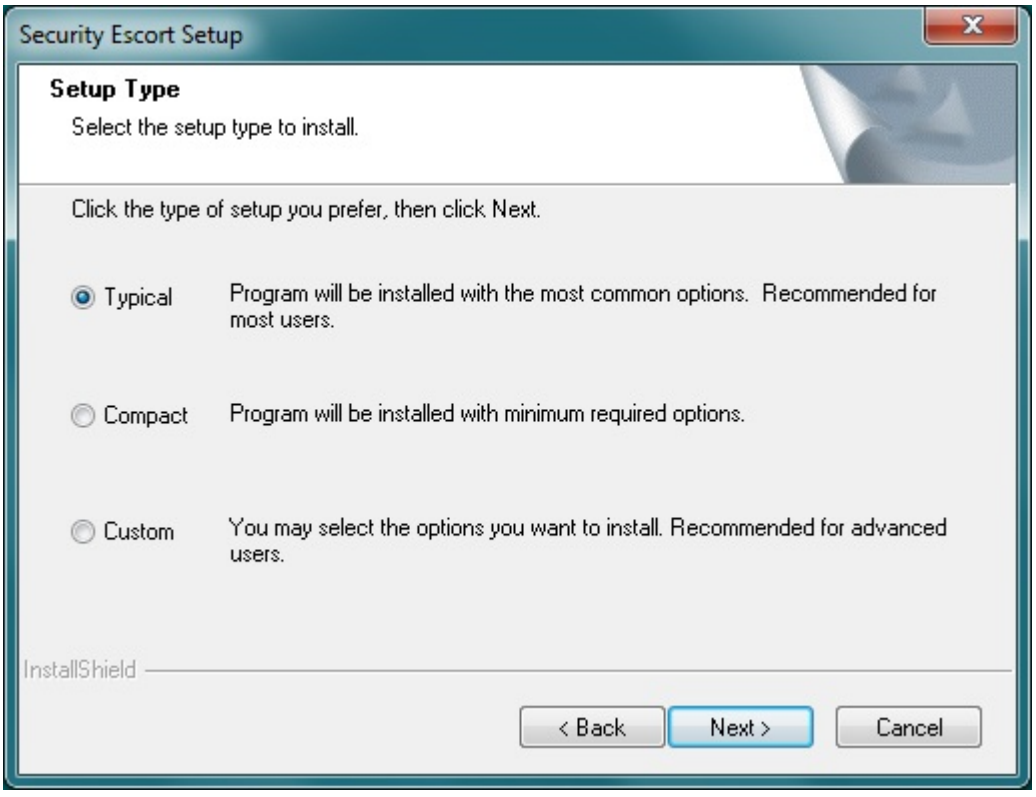

Security Escort Setup
Setup Type
Select the setup type to install.
Click the type of setup you prefer, then click Next.
Typical
Program will be installed with the most common options. Recommended for most users.
Compact
Program will be installed with minimum required options.
Custom
You may select the options you want to install. Recommended for advanced users.
InstallShield
< Back
Next >
Cancel

Figure 5.7: Setup Type Dialog

Select the type of installation you desire.

- **Typical** – For new installations, this is the option you should choose. It guarantees that all required components are installed and includes the installer for the software key. Use this selection for demo installations. Do not use this selection on existing installations; it replaces the databases and maps with the demo databases and maps.
- **Compact** – Only installs the application files. This selection can be used to update an existing installation. It does not write over the databases and map files. This selection cannot be used for new installations because it does not contain all required components, the installer for the software key, databases, and maps.
- **Custom** – This selection contains all systems components, databases, and maps. You may choose which to install.

Click the **[Next >]** button. The **Select Program Folder** dialog appears for you to place the Security Escort shortcuts in the selected program folder.

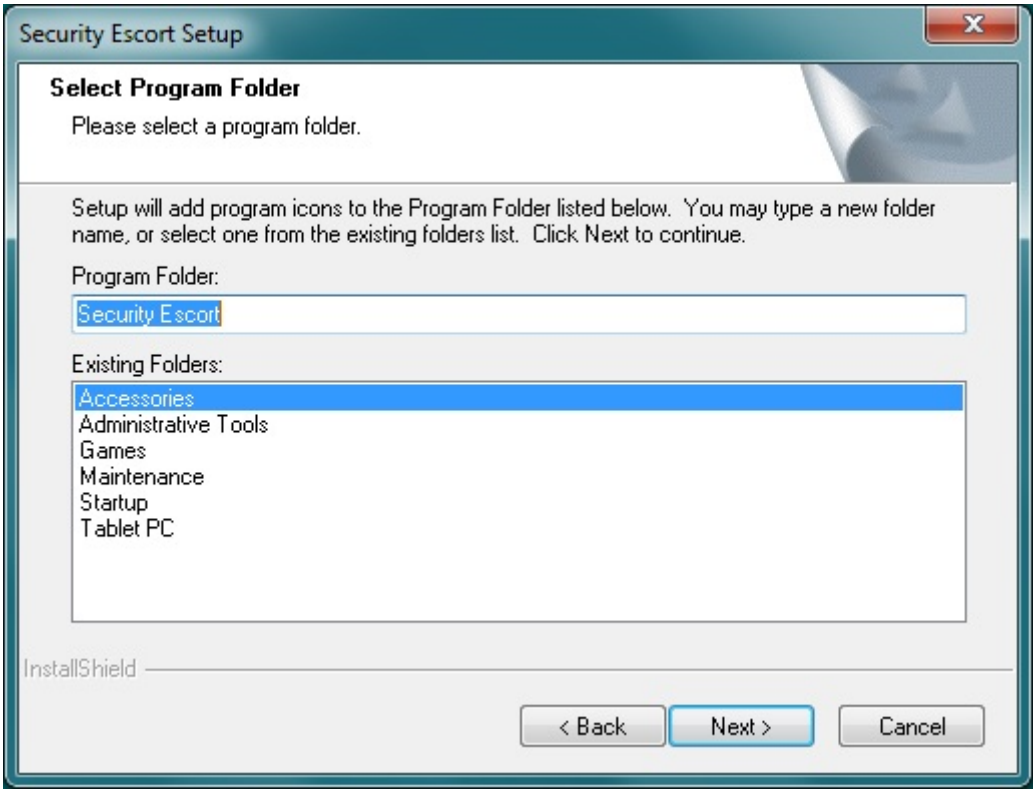


Figure 5.8: Select Program Folder Dialog

We are set to install the program. Click the **[Next >]** button. The installation starts, displaying the progress status.

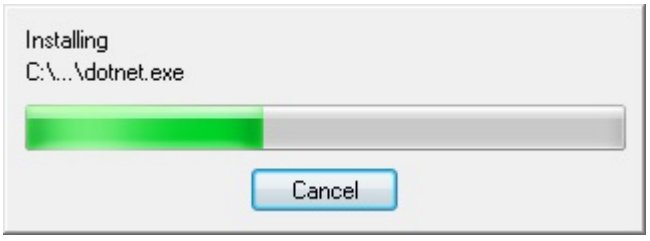


Figure 5.9: Installation Progress Dialog

Once installation has completed, the **Installation Complete** dialog appears, Click the **[Finish]** button to finish the installation.

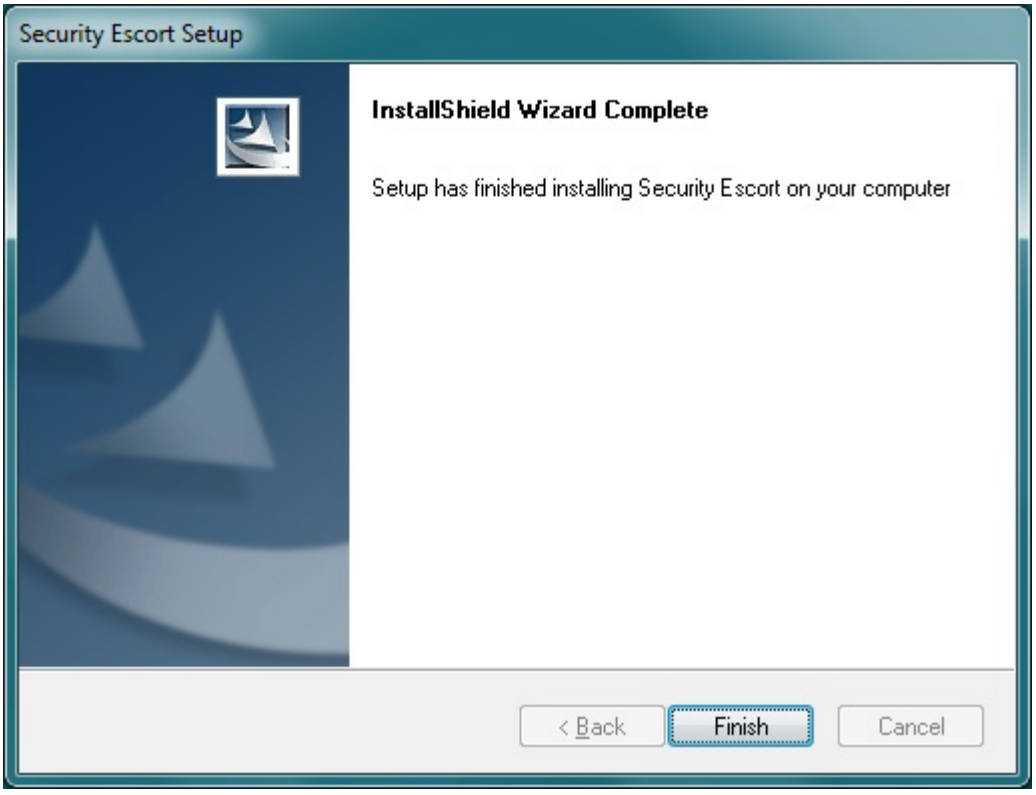


Figure 5.10: Installation Complete Dialog

To manually start the Security Escort program after installation, go to **Start > Programs > Security Escort**.
In a live system, it is recommended that the Security Escort program be configured to automatically start. To auto start the program, place a shortcut to ESC32.EXE (the Security Escort program, typically located in “C:\ESCORT”) in the following path:
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\Security Escort

Turning on Microsoft .NET Framework feature
After installing the Security Escort software, you need to turn on the .NET feature in order for the software to work. Go to **Start > Control Panel > Programs and Features**.

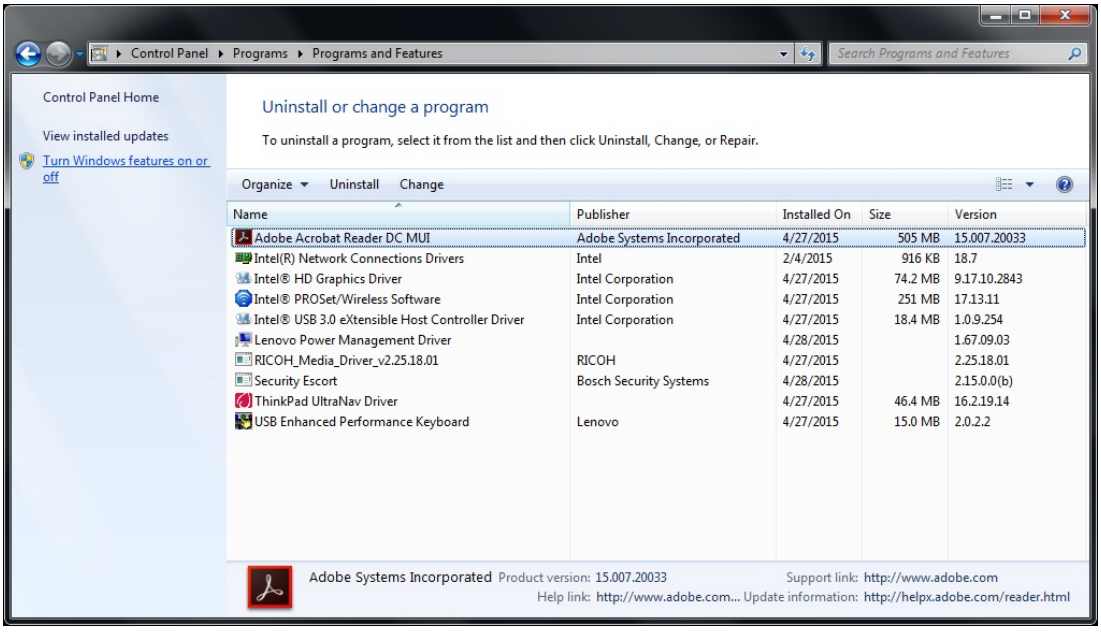


Figure 5.11: Control Panel

Click the **Turn Windows features on or off** link on the left of the window. The **Windows Features** dialog appears. Look for the **Microsoft .NET Framework 3.5.1** entry and ensure that the related checkboxes are selected.

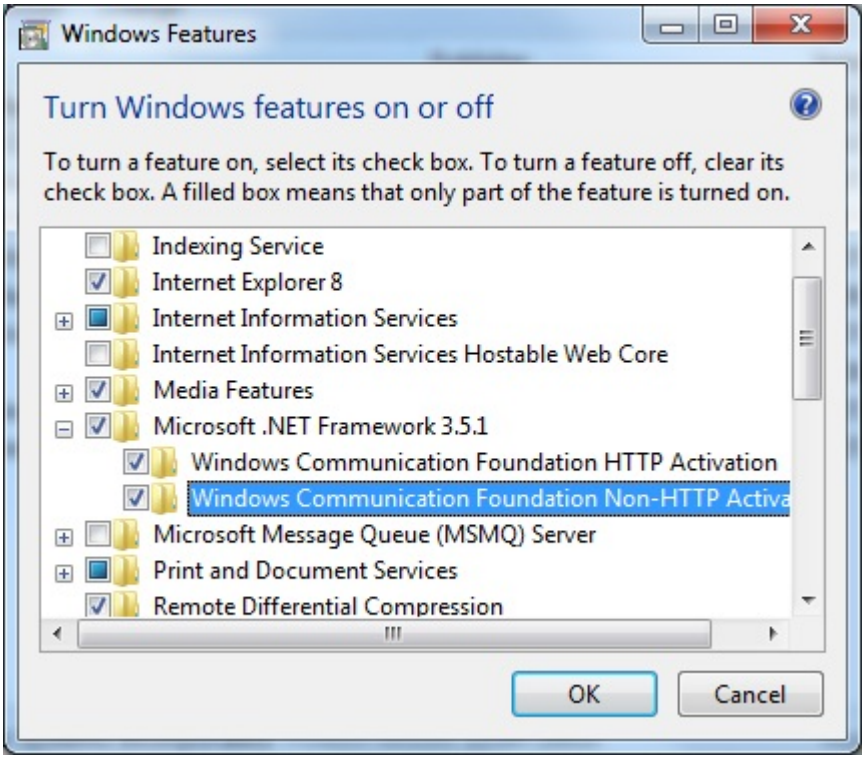

Windows Features
Turn Windows features on or off
To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.
Indexing Service
Internet Explorer 8
Internet Information Services
Internet Information Services Hostable Web Core
Media Features
Microsoft .NET Framework 3.5.1
Windows Communication Foundation HTTP Activation
Windows Communication Foundation Non-HTTP Activa
Microsoft Message Queue (MSMQ) Server
Print and Document Services
Remote Differential Compression
OK
Cancel

Figure 5.12: Windows Features Dialog

Click the **[OK]** button to turn on the Microsoft .NET Framework feature.

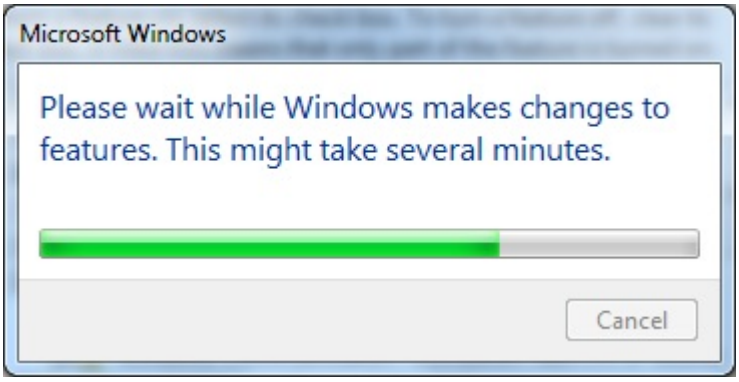


Figure 5.13: Change Progress Dialog

5.4.2 Image files

Map file generation and scaling

The Security Escort maps are standard Windows bitmap files (.BMP). MAP0.EDB is the default map file, usually the ground floor in multiple map systems. The map must be saved in the Security Escort subdirectory (typically “C:\ESCORT”). These maps may be created from scratch using any Windows paint program, however it is best to scan in an existing site map. Commercial copy centers usually have scanners that can handle larger drawing sizes.
If an AutoCad file is available, have AutoCad export a bitmap for the best looking maps that require the least work to make presentable. If the scale of the exported map is too large or too small, re-export the map at the corrected scale rather than scaling the map in a graphic editor. Scaling a bitmap file directly will produce a file that will require a significant amount of manual effort to make presentable.
Save the scanned image as a Windows bitmap file (.BMP) with 256 colors (8 bit color). High Color (16 bit) or True Color (24 bit) can also be used, but the file sizes will be much larger and the maps will be slower to load and may require more system RAM. It should be scaled so that the entire map file is at least 800 by 600 pixels (covering the entire Windows screen). The Security Escort software auto scrolls the map; therefore it is not a problem if the map is larger than the screen. The map should not be too large. There should be enough area of the map on the screen when an alarm is shown, so there is no question where in the facility the alarm is located from a quick review of the map. A good rule-of-thumb is 100 pixels would represent 15 m (50 ft) or greater.

Multiple map files

For a multi-story building, the maps for each floor must have the same resolution. Each map must be vertically aligned with all the floors above and below it. Therefore the maps will have the same origin (0,0 = upper left corner). Typically, you would do the map for the ground floor, then make the maps for the other floors by editing copies of the ground floor map.
Where transponders from multiple systems are reporting into the same computer, the map(s) for each system is separate and assigned unique map numbers, from the other maps on that same computer. The origin for the maps for each system is 0,0 = upper left corner. Therefore, the location of the receivers in the transponder database will only consider this system’s map without respect to the maps for any other systems being handled by the same computer.
The maps must be named MAP0.EDB, MAP1.EDB through MAP99.EDB. Where MAP0.EDB is the default map file, usually the ground floor. The Security Escort software shows the default map if there are no other events being processed at a given time.

Assign the desired map number to an area or point in the **Transponder Database**. Assign the map for a fixed location transmitter in the **Subscriber Database Advanced** dialog.

6 Central Console, computer setup and programming

6.1 Transponder comm port setup

Go to menu **Setup > Transponder comm port setup...** This dialog connects the communication port indexes set for each transponder in the **Transponder Database** to the physical communication ports on the computer.

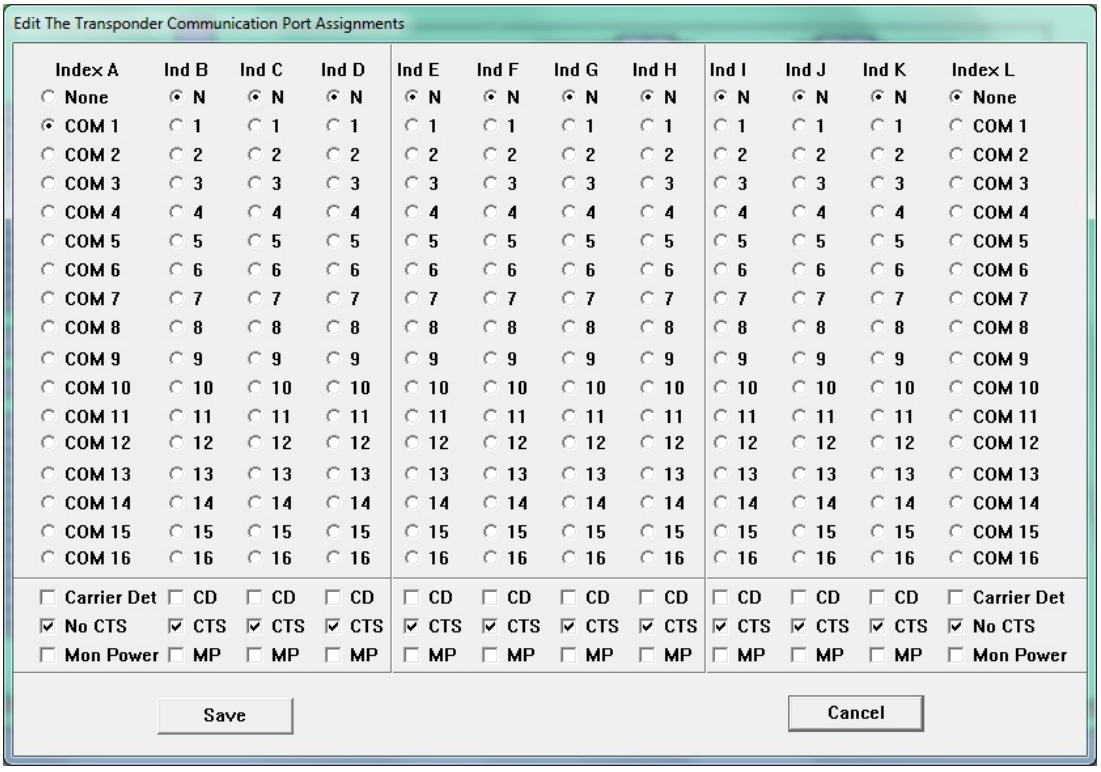


Figure 6.1: Transponder Comm Port Setup dialog

COM	The actual physical communication port over which communications to the transponder will be carried.
Carrier Det	If checked, verify that the communications port is not in use before communicating. Only to be used on half duplex links where Carrier Detect indicates that the link is in use. This setting is normally unchecked and rarely used.
No CTS	If checked, do not monitor the Clear to Send before communicating. This setting is normally checked.
Mon Power	If checked, monitor the Ring Indicator pin to indicate a remote power supply used on this communication link has not failed. This setting is normally unchecked.

6.2 Remote comm port setup dialog

This dialog connects the network, modem and system serial ports to the physical communication ports on the computer and sets their baud rate.

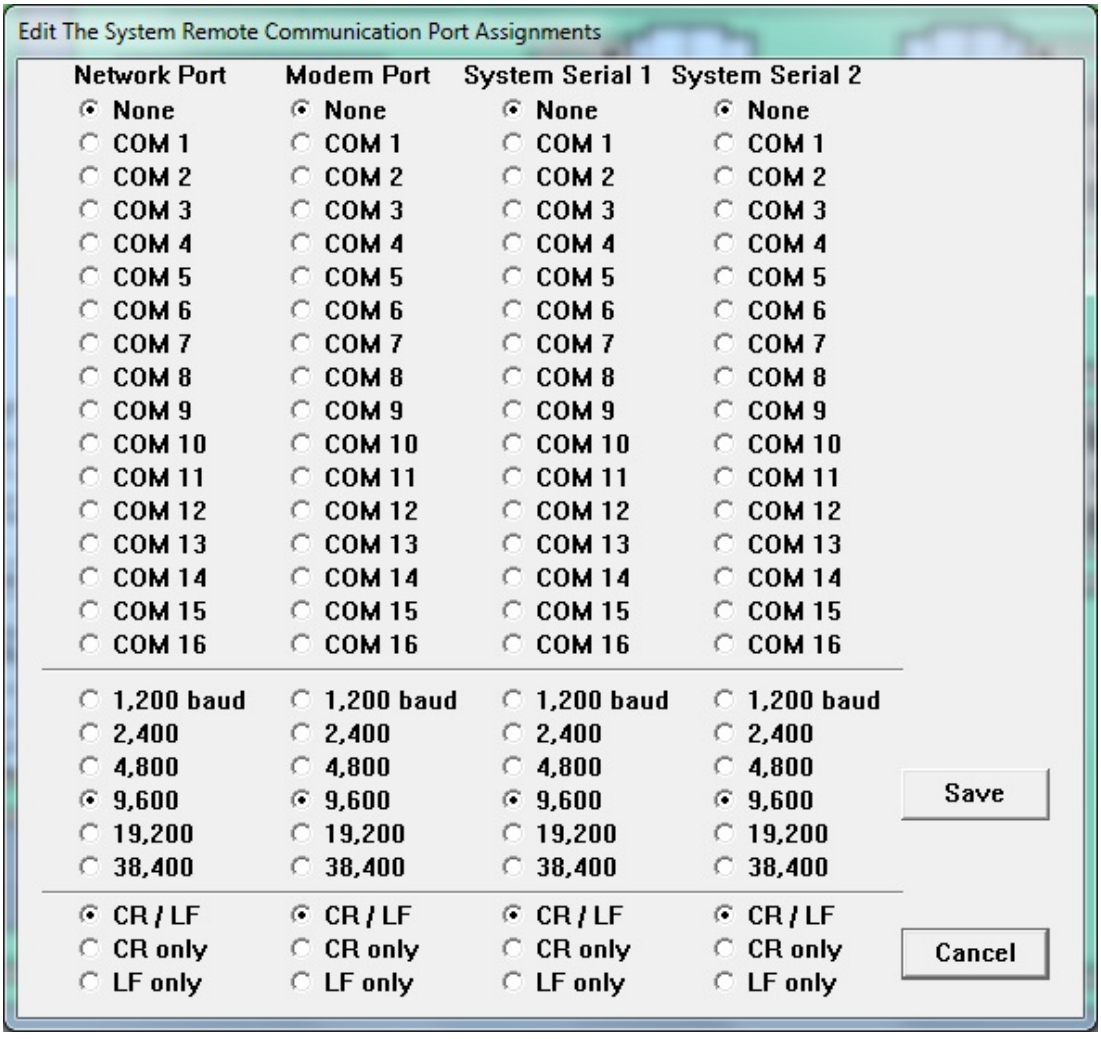


Figure 6.2: Remote Comm Port Setup Dialog

Network Port This port connects the master and slave computers of the Security Escort System. If this system has only a single computer, this setting should be set to none.

Modem Port This port typically connects to the modem for remote access and pager dial out. If set in the **Remote Setup** dialog, use this port without a modem for direct connection to a computer that is always on line.

System Serial 1/2 This is a general-purpose serial port. Its function is set up in the **Remote Setup** dialog.

COM The actual physical communication port over which these communications are carried.

Baud The speed at which characters are transmitted on this serial port. This setting must match the baud rate of the device connected at the other end of this serial connection. This setting should always be at the highest speed that both connected devices have in common. Modem connections are typically much more efficient, if the baud rate is set significantly faster than the modems rated speed (for a 28.8 modem, set the baud rate to 57600 or 115200). The default setting is 9600 baud.

CR/LF Appends carriage return and line feed characters at the end of each string transmitted (default). Only functions with the system serial ports (ignored on the network and modem ports).

CR Only Appends a carriage return character at the end of each string transmitted. Only functions with the system serial ports (ignored on the network and modem ports).

LF Only Appends a line feed character at the end of each string transmitted. Only functions with the system serial ports (ignored on the network and modem ports).

6.3 Remote setup dialog

This dialog sets up the remote access and system serial port parameters.

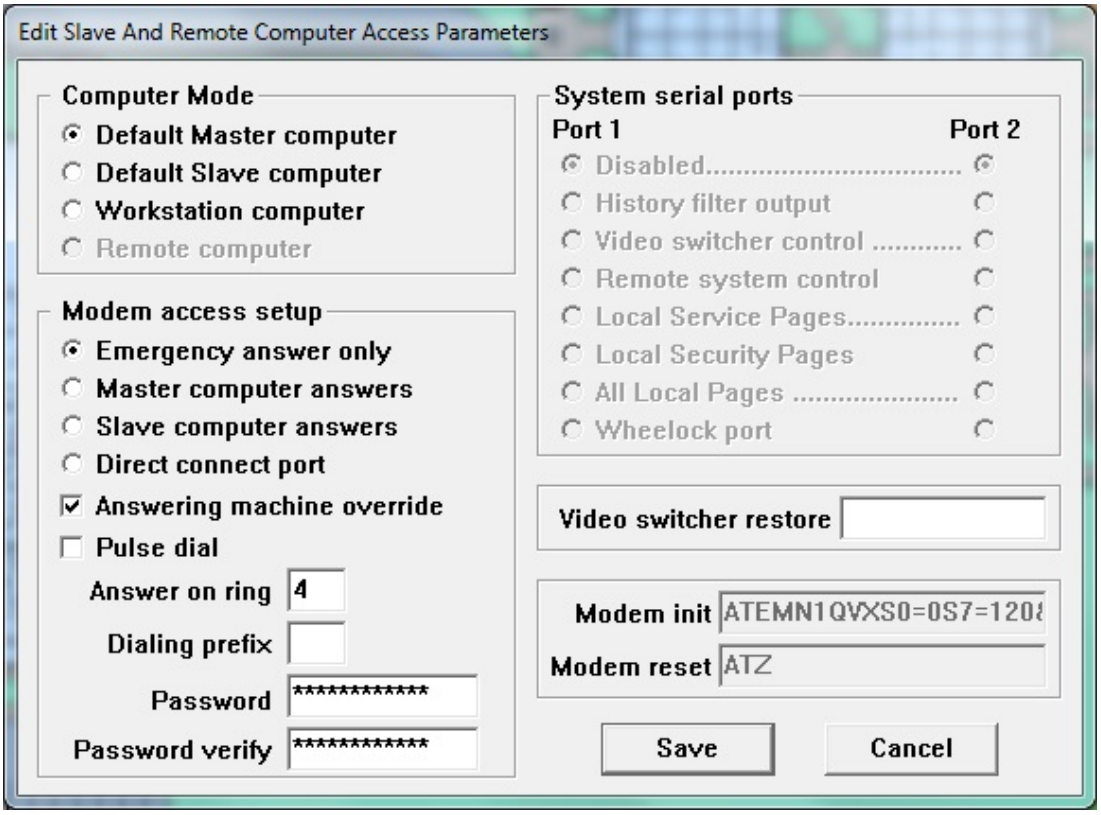


Figure 6.3: Slave and Remote Computer Access Parameters Dialog

Default Master computer	This computer is either the only computer in the system, or on startup, this computer defaults to the Master computer in a live Security Escort System.
Default Slave computer	On startup, this computer defaults to the slave computer in a live Security Escort System.
Workstation computer	This computer is used in a live Security Escort System for all operator functions. It cannot control the system like the Master and Slave computers.
Remote computer	This computer is not in a live Security Escort System. It is used only for remote access. For this setting to be enabled, all transponder communication ports and the network port must be set to “None”.
Emergency answer only	Allows the Master computer to answer a remote access only after 10 rings. If the Master does not answer, the Slave answers after 12 rings.
Master computer answers	Allows the Master computer to answer a remote access after the programmed number of rings. If the Master does not answer, the Slave will answer after the programmed number of rings plus 2.
Slave computer answers	Allows the Slave computer to answer a remote access after the programmed number of rings. If the Slave does not answer, the Master answers after the programmed number of rings plus 2. Generally, it is better to have the Master computer answer remote access calls.
Direct connect port	The modem port is not connected to a modem. This setting will allow a direct connection to another computer. This additional computer will not display alarms, but otherwise will behave like a Slave computer.
Answering machine override	If checked, an answering machine is connected to this phone line. If the answering machine answers a remote access call, hang up and redial. When another call is received within 1 min. of the last ring of a previous call, the Security Escort System will answer on the first ring, overriding the answering machine.
Pulse dial	If checked, use pulse dial on all outgoing calls. Otherwise, tone dialing (default) is used.
Answer on ring	Program the number of rings on which to answer. If there is an answering machine on this phone line, set the number of rings to at least 2 greater than the number of rings the answering machine answers. Also check the **Answering Machine Override** checkbox.
Dialing prefix	On outgoing calls, enter the dialing prefix, if any.

Password	This is the password that is used to gain remote access to the Security Escort System. If the first 5 characters of the password match the remote systems password, read only access will be allowed. If the first 8 characters match, you will be allowed to edit databases remotely (not currently implemented). If all 12 characters match, you will also be allowed to change system parameters remotely.
Password verify	For verification, reenter the same password as above.
Disabled	If selected, this system serial port is disabled (default).
History filter output	If selected, this system serial port sends out whatever items that are selected in the **History Filter** dialog.
Video switcher control	If selected, this system serial port sends out the strings programmed in the **Video Switcher** field of the **Transponder Database Edit** dialog's **Area** data. Also see **Video switcher restore** field below.
Remote system control	If selected, this system is controlled by another system through a proprietary protocol. This setting can only be used when two systems are specifically designed to work together.
Local Service Pages	If selected, system will send service pages via the local port.
Local Security Pages	If selected, system will send security pages via the local port.
All Local Pages	If selected, system will send both service and security pages via the local port.
Video switcher restore	This string is transmitted on any system serial port programmed for **Video switcher control** when all alarms are restored. This string is transmitted to the video switcher to reset it to the default displays. Up to 20 characters can be entered. Control characters can be entered as [^][A] for control A.
Modem init	This is the initialization string transmitted to the modem to set it up for all communications except paging. Normally, this setting does not need to change. To allow changes to this string, hold down the <Shift> + <Ctrl> keys when this dialog is first opened. This string is specific to each modem model. The default string should work with most modems.
Modem reset	This is the reset string transmitted to the modem. Normally, this setting does not need to change. To allow changes to this string, hold down the <Shift>+ <Ctrl> keys when this dialog is first opened. This string is specific to each modem model. The default string should work with most modems.
[Save]	Save the changes and close the dialog window.
[Cancel]	Cancel the changes and close the dialog window..

6.4 Transponder Database

The **Transponder Database** is established at system set-up and contains all necessary configuration data for each transponder, receiver and alert unit. It describes the basic structure of the installation, including all device names, locations, types, multiplex addresses, etc. This information is used by the Central Console to generate “Alarm” and “Test” displays on the Console and in determining which alert units are to be activated. Access to the **Transponder Database** is from the **File** menu on the main menu bar. The following paragraphs describe the elements of the **Transponder Database** dialog.

6.4.1 Transponder information sheet

Transponder Number:		**Transponder Location:**	
Transformer for Transponder Location:			
Breaker Panel Location:		**Breaker Number:**	
Siren/Strobe Output To:			
Keyswitch Monitoring To:			
Bus #0 Locations:			
Point #0:			
Point #1:			
Point #2:			
Point #3:			
Point #4:			
Point #5:			
Point #6:			
Point #7:			
Bus #1 Locations:			
Point #0:			
Point #1:			
Point #2:			
Point #3:			
Point #4:			
Point #5:			
Point #6:			
Point #7:			
Bus #2 Locations:			
Point #0:			
Point #1:			

Point #2:	
Point #3:	
Point #4:	
Point #5:	
Point #6:	
Point #7:	
Bus #3 Locations:	
Point #0:	
Point #1:	
Point #2:	
Point #3:	
Point #4:	
Point #5:	
Point #6:	
Point #7:	
Bus #4 Locations:	
Point #0:	
Point #1:	
Point #2:	
Point #3:	
Point #4:	
Point #5:	
Point #6:	
Point #7:	
Bus #5 Locations:	
Point #0:	
Point #1:	
Point #2:	
Point #3:	
Point #4:	
Point #5:	

Point #6:	
Point #7:	
Bus #6 Locations:	
Point #0:	
Point #1:	
Point #2:	
Point #3:	
Point #4:	
Point #5:	
Point #6:	
Point #7:	
Bus #7 Locations:	
Point #0:	
Point #1:	
Point #2:	
Point #3:	
Point #4:	
Point #5:	
Point #6:	
Point #7:	
Location of Splices:	

6.4.2 Transponder Database dialog

The **Transponder Database** is established at system set-up and contains all necessary configuration data for each transponder, receiver and alert unit. It describes the basic structure of the installation, including all device names, locations, types, multiplex addresses, etc. This information is used by the Central Console to generate alarm and test displays on the Central Console and in determining which alert units are to be activated.

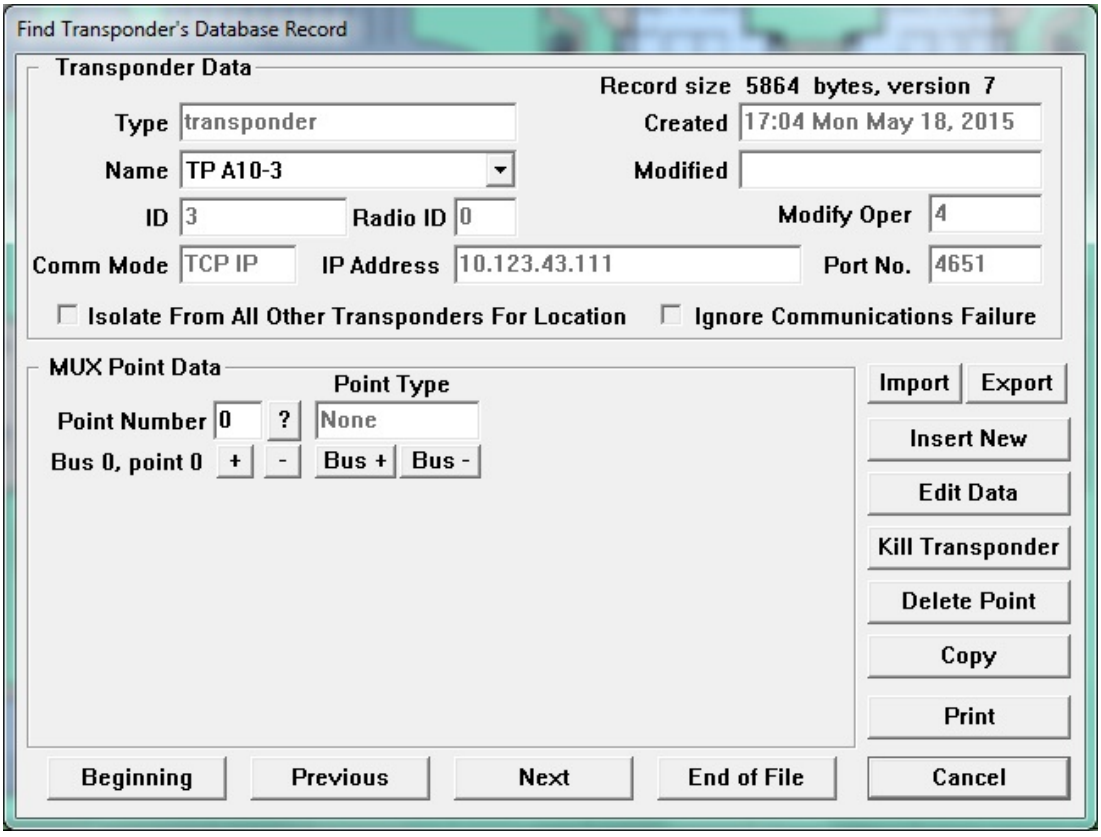


Figure 6.4: Find Transponder's Database Dialog

Access the **Transponder Database** from the **File** menu on the main menu bar. The following table describes the elements of the **Find Transponder's Database Record** dialog.

Type	This field indicates the type of transponder record that you are currently viewing. Currently, there is only one type of transponder available.
Name	This drop-down list contains the names of the transponders. Selecting the name of the transponder in the drop-down list displays information of the transponder record in the dialog window. The transponder names are assigned during set-up and are used to indicate the physical location of the transponder, or the region of the protected area covered by a particular transponder.

Created **Modified** **Modify Oper**	The system software automatically creates these 3 fields to the right of the **Find Transponder's Database Record** dialog. They represent the date the transponder was first entered into the **Transponder Database**, the date of the last change of any entry for this transponder, and the identity of the operator making the last change (determined from the password entered to make the change).
ID	This is a number assigned to the transponder at system set-up. It is used by the Central Console to identify the transponder during all communications between the Central Console and the transponder. The number must agree with the transponder address, which is set during final installation using switches on the transponder circuit board. **Note: The number 0 is not allowed as a transponder address.**
Radio ID	This is the identification number for the radio interface unit, if the transponder communicates to the Central Console by means of a radio link. (This feature is currently not implemented)
Comm Mode	This indicates which communication mode that the Central Console is using to communicate with the transponder.
IP Address	If the **Comm Mode** is "TCP IP", this field will appear in the dialog window. This field indicates the IP address assigned to the transponder.
Port No.	If the **Comm Mode** is "TCP IP", this field will appear in the dialog window. This field indicates which Central Console communications port will be used to communicate with this transponder.
Comm Port Index	If the **Comm Mode** is "RS232", this field will appear in the dialog window. This field indicates which Central Console communications port will be used to communicate with this transponder. The **Transponder Comm Port Setup** dialog selects the specific physical port that this index will refer to.
Isolate From All Other Transponders For Location	When checked, this transponder is isolated from all other transponders for location considerations. This should be used when distant transponders sometimes hear an alarm and throw off the alarm location calculation. If this checkbox is checked, it indicates that this transponder is protecting an area that is independent of all other transponders in the system. When an alarm is reported, and receivers on this transponder have the best reception, only the receivers on this transponder will be considered for the location of this alarm. If another transponder has the best reception, then the receivers on this transponder will be ignored for the location of this alarm.

Ignore Communications Failure	This checkbox allows communications failures to be ignored for this transponder. It is used during a new installation for transponders that are not yet fully on line. During system maintenance, when a transponder is out of service for a while, it is used so that the communications failure messages will not flash on the screen and distract the operator. **Checking this checkbox causes the system to ignore communication failure. Therefore, if communications fail with this transponder, the area this transponder protects will not be protected, and alarms from subscribers in that area will be missed without the operator's knowledge. This checkbox should not be checked in a live system.**
[Insert New]	Clicking this button displays a new **Edit Transponder's Database Record** dialog window. This is used to enter a new transponder to the database.
[Edit Data]	Clicking this button allows the currently displayed transponder's database record to be modified.
[Kill Transponder]	Clicking this button deletes the currently displayed transponder's database record. If the transponder is "killed", its data is permanently deleted and cannot be recovered.
[Delete Point]	Clicking this button deletes the currently displayed point from the current transponder's database record. If the point is deleted, its data is permanently deleted and cannot be recovered.
[Copy]	Clicking this button copies the currently displayed transponder's database record into a new transponder record. This allows similarly configured transponders to be programmed once then copied into a new record. **Note: It is not possible to edit the Transponder ID itself. If this should be necessary, the [Copy] button can be used to produce another Transponder Database entry duplicating the first, but with the Transponder ID blank. The new Transponder ID can be entered, the new data saved by using the [Save] button, and the old transponder entry can be deleted using the [Kill Transponder] button.**
[Print]	Clicking this button prints the currently displayed transponder's database record.
[Beginning]	Clicking this button changes the currently displayed transponder to the first transponder in the database.
[Previous]	Clicking this button changes the currently displayed transponder to the previous transponder in the database.
[Next]	Clicking this button changes the currently displayed transponder to the next transponder in the database.
[End of File]	Clicking this button changes the currently displayed transponder to the last transponder in the database.

MUX Point Data

The lower section of the **Find Transponder's Database Record** dialog window provides information on the devices controlled by the selected transponder record.

Two digits represent each receiver or alert unit address. The first is the number of the multiplex bus on which the device is mounted (0 to 7) and the second is the multiplex point address assigned to the particular device. On each of the eight multiplex busses, up to 8 devices may be installed, but each device must be assigned a unique multiplex point address (0 to 7). More than one device can have a particular multiplex point address, but only on different busses. The multiplex point addresses are assigned by switch settings on the device (receiver or alert unit) circuit boards. These multiplex point address settings are also a part of the **Transponder Database**. The multiplex address shown in the **Transponder Database** and the multiplex address set on the device circuit board must agree. The **Transponder Setup** dialog is used to verify multiplex address settings.

Notice!

It is a good idea to create an entry in the **Transponder Database** for each transponder in the system before entering the data for each device, so that all transponders appear in the drop-down menus.

6.4.3 Creating a new transponder entry

Creating and modifying the **Transponder Database** requires special authority levels usually assigned only to the installing company's personnel. Clicking the **[Insert New]** button opens a new **Transponder Database** dialog window.

The **System Design Layout Sheets** prepared in advance by the installation manager should contain the necessary information for assigning the **Transponder Name** and **ID**, the **Comm Port** or **Radio ID**, as well as the names and multiplex addresses for all receivers and alert units connected to each transponder. The layout sheets will also contain the text to be used to indicate the receiver locations and will designate the alert units to be driven by each receiver.

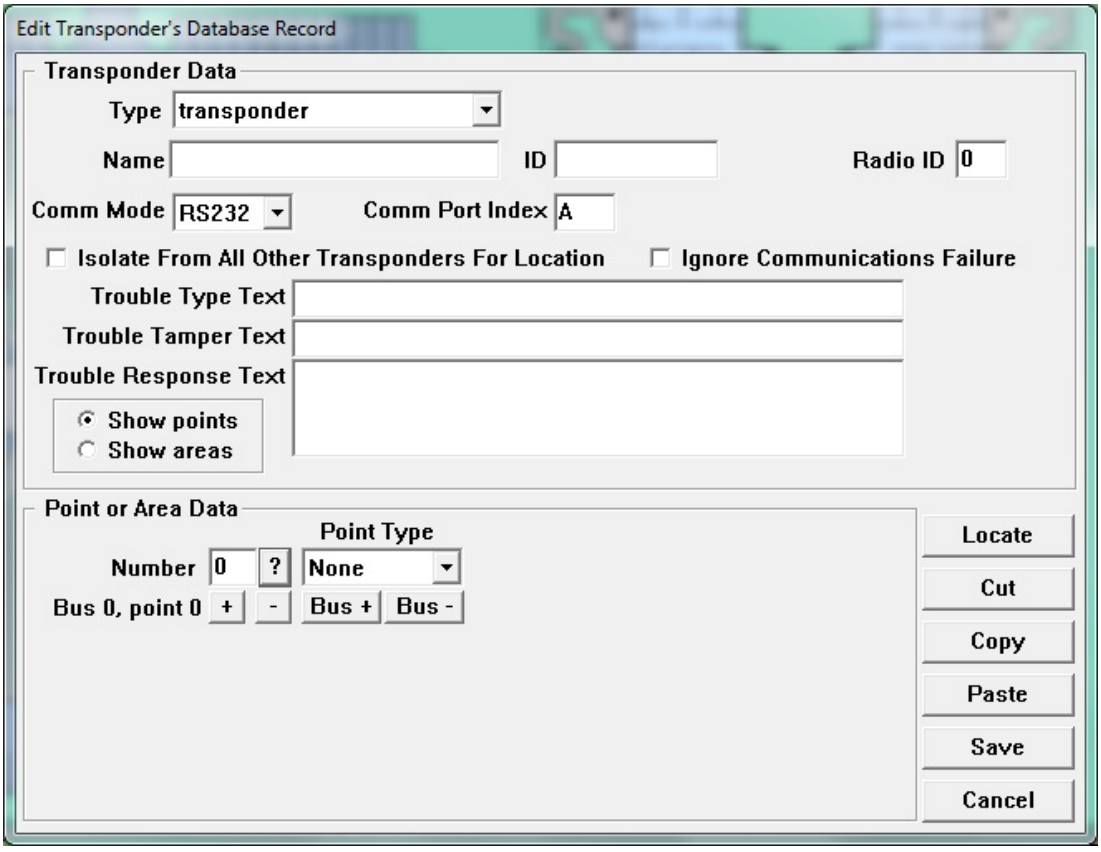


Figure 6.5: Blank Dialog Resulting from Selection of [Insert New] Button

The new elements of the **Edit Transponder's Database Record** dialog.

Trouble Type Text	This is the text that will be shown in the trouble dialog when the remote key input on the transponder goes active (shorted).
Trouble Tamper Text	This is the text that will be shown in the trouble dialog when the remote key input on the transponder goes into trouble (open).
Trouble Response Text	This is the text that will be shown in the trouble dialog as the response test. The actions the responding individual should take.
Show Points	If selected, the lower section of the **Transponder Database** dialog will show the point's (receiver, virtual receiver or alert unit's) database values.
Show Areas	If selected, the lower section of the **Transponder Database** dialog will show the alarm area's database values.

6.4.4 Modifying existing transponder entry

If the transponder is already defined in the **Transponder Database**, the **[Edit Data]** button is used to complete or modify the data. The data that can be modified is the same when creating a new transponder entry (see *Creating a new transponder entry, page 82*).

6.4.5 Setting receiver parameters

Create or modify the receivers of the transponder using the features of the **Point** or **Area Data.** For configuring **Area Data**, refer to the *Alarm area setup* section. The sections below explain how to configure the receiver points for the transponder.

Entering point number

Each receiver and alert unit connected to the transponder has a unique **Point Number** assigned during the system design process. This **Point Number** ranges from 0 to 63, and corresponds to a specific bus number and point multiplex address number. The multiplex address, set by means of switches on the device (receiver or alert unit) itself, must correspond with the **Point Number** assigned in the **Transponder Database**.

There is a one-to-one relationship between the **Point Number** and the combination of **Multiplex Point Address** / **Bus Number** pair. For example, a device programmed with **Multiplex Point Address** location 3 on **Bus Number** 5 would correspond to the **Point Number** 29.

Clicking the **[?]** button to the right of the **Point Number** text box opens a dialog window displaying the **Point Number** in a table. Clicking on any **Point Number** in the table automatically closes this window and fills the number in the **Point Number** field on the **Transponder Database** dialog. The **Bus number** and **Point address** are also changed to reflect the selection.

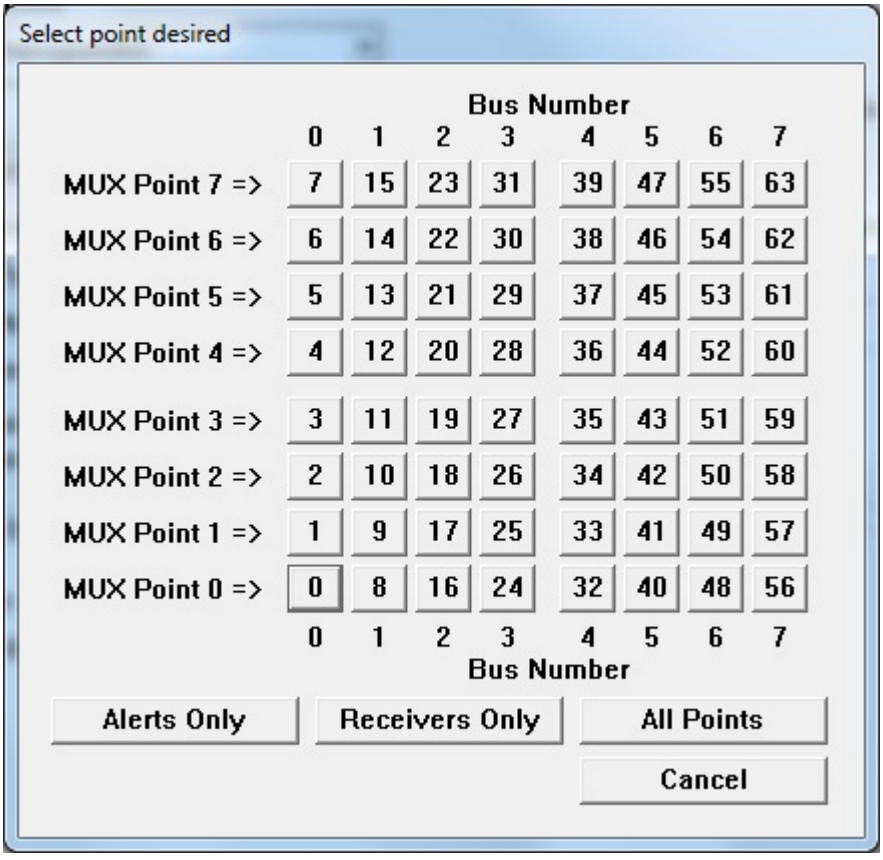


Figure 6.6: Select Point Dialog with "All Points" Selected

This table provides a quick way to select a particular device without having to translate between the two numbering (**Bus Number/Point Address**) systems. The three buttons at the bottom of this dialog allow the user to display:

1. all possible device numbers (**[All Points]** button) regardless that the particular transponder has a device assigned to the number,
2. only locations populated by receivers (**[Receivers Only]** button), or
3. only locations populated by alert units (**[Alerts Only]** button).

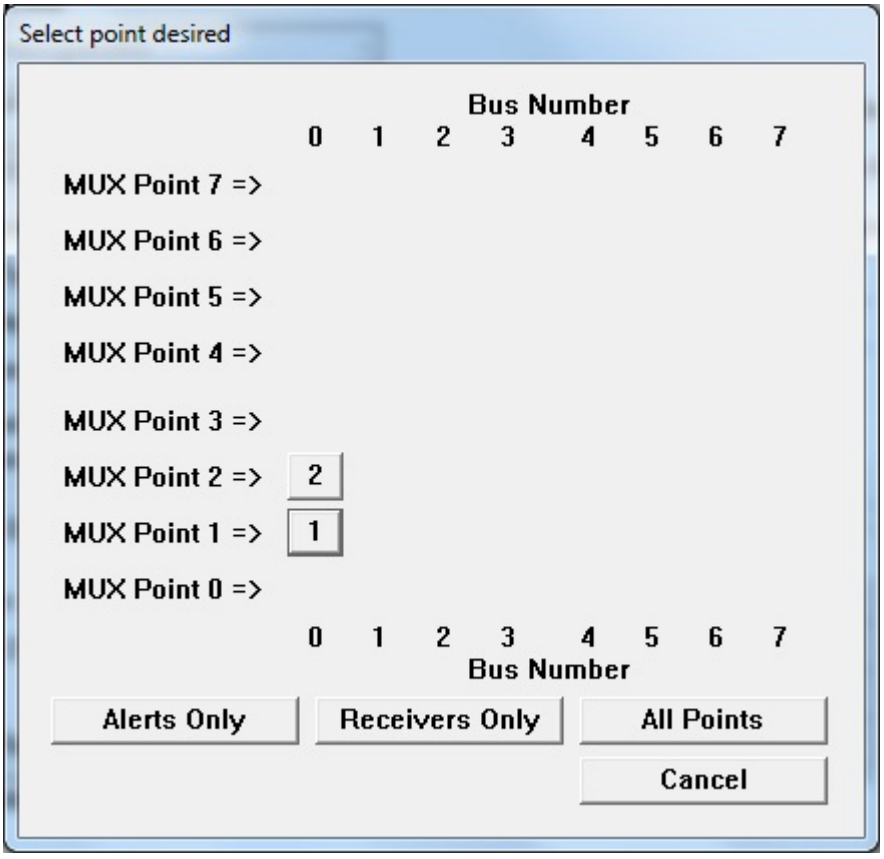


Figure 6.7: Select Point Dialog with "Receivers Only" Selected

Alternatively, the **[+]**, **[-]**, **[Bus +]** and **[Bus** –] buttons, just below the **Point Number** and **Point Type**, allow the user to quickly advance the device selection by one location, either one **Point** location (**[+]** or **[-]**) or one **Bus** number (**[Bus +]** or **[Bus -]**). This is useful when a task requires proceeding from device to device, as during system setup or check out. The **[?]** button is used to display all devices to facilitate quick selection of a particular device. It is most useful when diagnosing a problem with a particular device.

Selecting the Point Type

The **Point Type** drop-down list indicates the type of device at the location currently selected in the **Point Number** field. Once the **Point Number** text box contains the proper value, the device type can be selected from the **Point Type** drop-down list.

Figure 6.8: Drop-Down List for Selection of Point Type

The valid point types are “receiver”, “Alert unit”, “Virtual” receiver, and “None”. Select the **Point Type** device accordingly when there is a physical device connected at this bus location.

Selecting “receiver” as the Point Type

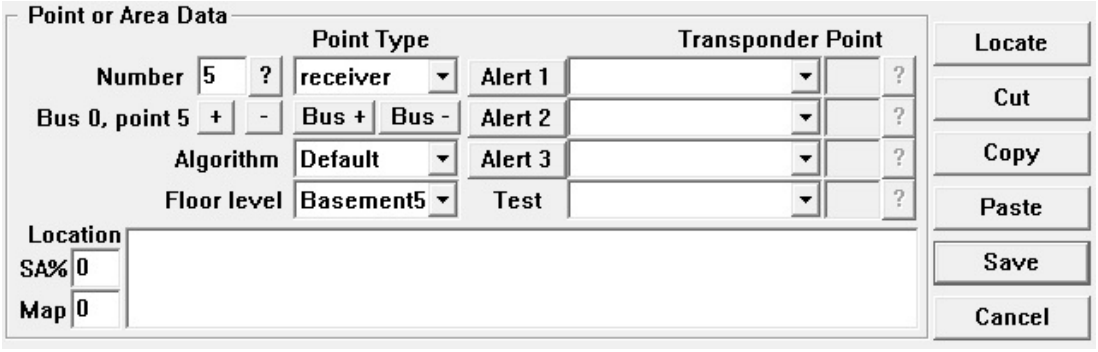


Figure 6.9: Data Entry after Selection of Receiver Point Type

Each receiver can be assigned up to three alert units that are to be activated if it is one of the receivers reported by the transponder as part of an “Alarm” event. Each receiver can also be assigned one alert unit that is to be activated to confirm “Test” transmissions. These alert units need not be connected to the same transponder as the receiver.
To assign alert units to each receiver, the drop-down lists of **Alert 1**, **Alert 2**, and **Alert 3** fields are used to select the transponder of the designated alert unit. The point number can be keyed into the **Point** text box, or click the **[?]** button to display the receiver selection table. Click the receiver number on the selection table dialog to populate the **Point Number** in the **Point** text box.
Similarly, any alert unit, whose strobe unit is to be activated in the event of a “Test” transmission from a transmitter, can be assigned using the drop-down lists of **Test** field.

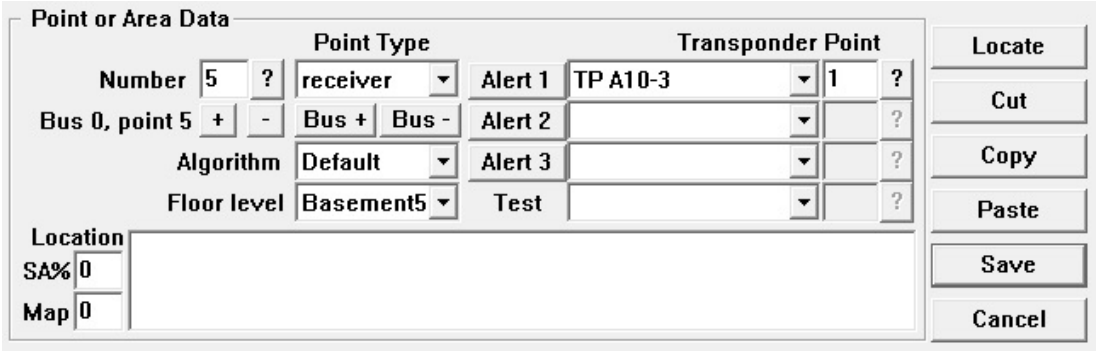


Figure 6.10: Assigning Alert Unit to Receiver Point Type

Use the **Floor Level** drop-down list box to assign the physical floor level where a receiver is mounted at.
The **Location** field contains the text to be displayed on the Alarm Screen, if this receiver is one of those closest to the alarm source. The description is developed with the guidance of the security personnel who must respond to an alarm. It is vital that the description be clear and unambiguous to them.
To enter a location description, place the cursor in the **Location** field, click the mouse, and begin typing. Receiver and alert unit location names are important because they are used for directing response to an alarm and aid service personnel in identifying the device in the event of a problem. The Problem Reports displayed on the central console and printed by the hardcopy printer contain the device location descriptions that are entered in the **Location** field.

The **Map** field defines which bitmap to display for this receiver or area when an alarm is closest to it. The default map is 0, which corresponds to bitmap MAP0.EDB stored in the Security Escort sub-directory. Map 1 is MAP1.EDB. There can be 100 maps per Security Escort System (0 to 99).

Selecting “Virtual” receiver as the Point Type
Use the “Virtual” selection when there is no physical device connected at this bus location. Starting with version 2.03 of the Security Escort software, you can add “Virtual” receivers in the **Transponder Database**. A “Virtual” receiver is added at one of the 64 points allowed per transponder. However, there is no physical hardware used.

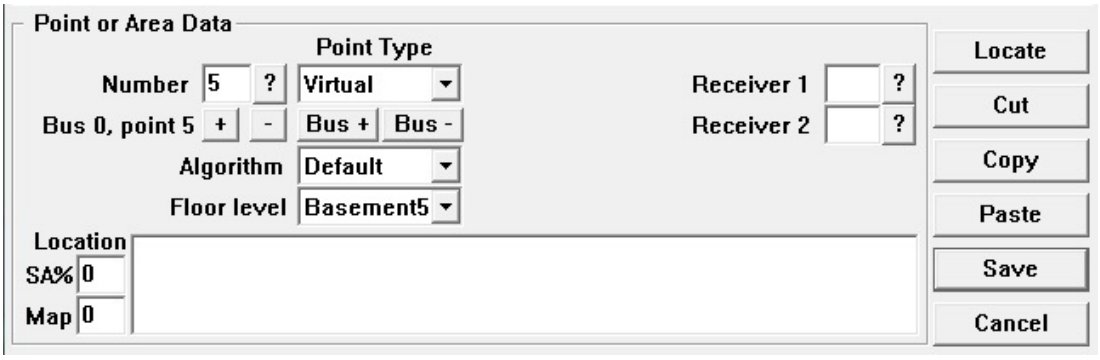


Figure 6.11: Data Entry after Selection of Virtual Receiver Point Type

The “Virtual” receiver is intended to compensate in cases where there is a receiver imbalance. For example, if a building with a dense population of receivers is adjacent to a fence with few receivers and an alarm occurs between them; the alarm location may pull towards the building. The “Virtual” receiver references two other physical receivers that must be on the same transponder. Only if both of the referenced receivers receive an alarm transmission, then the “Virtual” receiver will be added to the alarm as if was a physical receiver that heard the alarm at the average receive level of the 2 referenced receivers.
Both the referenced receivers are configured in the **Receiver 1** and **Receiver 2** fields. These are the two receivers, on the same transponder, that a “Virtual” receiver assumes the average of. Both receivers must receive a signal before the “Virtual” receiver reports it also received a signal that is the average of the other two receivers signals. The location algorithm and sensitivity adjust work the same for a “Virtual” receiver as for a physical receiver. Enter the receiver’s **Point Number** in the fields, or click the **[?]** button to select the receiver accordingly. The “Virtual” receiver’s location and sensitivity may be adjusted the same as a physical receiver. After a “Virtual” receiver is added, verify the surrounding areas to make sure they have not been adversely affected. **In no event should a “Virtual” receiver be utilized as a cost savings measure to avoid the installation of an actual receive**r.
For explanations of **Floor level**, **Location** and **Map** fields, please refer to section *Selecting “receiver” as the Point Type***.**

Selecting the algorithm
Starting with version 2.03 of the Security Escort software, there are 5 different location algorithms that can be selected on an individual receiver basis in the **Transponder Database**. “Classic” (original Security Escort algorithm), “Linear”, “Low” pull, “Medium” pull and “Strong” pull. By default when a receiver is set for outside or tunnel, it will use the “Linear” algorithm and all other receivers will use the “Low” pull algorithm. The receiver that hears the alarm transmission the strongest will determine the algorithm used for this alarm.

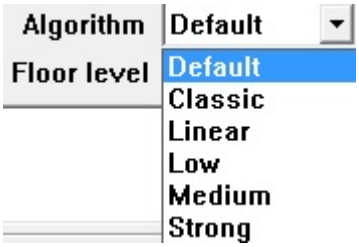


Figure 6.12: Location algorithm selection

Changing the algorithm setting for a receiver only affects the location when the alarm is close to this receiver and it hears the alarm the strongest. The stronger the pull the more the alarm will be pulled towards the receiver, with linear having no extra pull.
The algorithm setting will only be available if the **Enable algorithm tweaks** checkbox is checked in the **System Preferences** dialog. Also starting with version 2.03 of the Security Escort software, individual receiver sensitivity can be set in the **Transponder Database**. Receivers can be adjusted from 50% to 149% of their normal sensitivity using the **SA%** setting.

Adjusting the Sensitivity (SA%)
Security Escort software version 2.03 and higher allow individual receiver sensitivity to be set in the **Transponder Database**. Receivers can be adjusted from 50% to 149% of their normal sensitivity. No physical receiver changes or upgrades are required. This setting should only be changed if there are known location accuracy problems in the area of this receiver. Settings of 50 to 99 desensitize the receiver to 50% to 99% of the actual received signal strength. Settings of 1 to 49 increase the sensitivity to 101% to 149% of the actual received signal strength. Try changing the sensitivity of receivers one at a time while testing the alarm location response. For example, if alarms are being pulled towards a particular receiver, lower its sensitivity in 10% increments and retest. If the area can be corrected using this method, verify the surrounding areas to make sure they have not been adversely affected. Generally, it is better if the correction is done in small steps while verifying the adjacent areas, rather than trying to correct the entire error in one step.
The **SA%** option is only available if the **Enable algorithm tweaks** checkbox is checked in the **System Preferences** dialog. Also in the **Transponder Database**, the **Algorithm** dropdown list allows selection of “Default”, “Classic”, “Linear”, “Low”, “Medium” or “Strong” pull location algorithms for each transmitter. The point reporting the best reception level determines the actual algorithm used for the location on any event. If programmed as “Default”, the algorithm used is “Linear” for points programmed as outdoor or tunnel. All other points use “Low”. If the point reporting the best reception level is not programmed for the “Default” algorithm, the location calculation uses the algorithm programmed.

Other miscellaneous command buttons
The functions of the other miscellaneous command buttons are as of below:

[Locate] When clicked, the **Edit Transponder's Database Record** dialog disappears and the cursor changes to a cross hair. Moving the cursor to a point on the map and clicking the left mouse button scrolls the map so the point is at the center of the screen and all previously defined receivers and areas are shown with numerical labels.
When the map is showing the location of the desired receiver, move the cross hair to the exact location of the receiver and click the right mouse button. The **Edit Transponder's Database Record** dialog reappears and the selected location is entered into the X and Y coordinates.
When the map shows the desired location, move the cross hair to the exact location of the first point of the polygon that describes the boundary of the area and right click. Move the cursor to the second point of the polygon and again right click. The computer draws a straight line between the first and second points. Repeat this process drawing all sides of the polygon to define the area. To close the polygon, place the last point on top of the first point. The polygon can have up to nineteen sides and no two lines of the polygon may cross each other. If you try to create more than nineteen sides, the computer automatically closes the polygon with the nineteenth side. When the polygon is closed, it can be crosshatched to make it more visible. After the polygon is complete, double click the left mouse button to return to the **Edit Transponder's Database Record** dialog.
If the area being defined is a virtual monitor "fence" area for wandering alarms, the monitor fence (area boundary) should be drawn at least 7.62 m (25 ft) past the area to be protected to reduce potential false alarms. This is due to the basic location accuracy of the Security Escort system.
If the cross hair cursor is displayed and you want to exit without changing any coordinate values, press the <Esc> key and the **Edit Transponder's Database Record** dialog reappears.

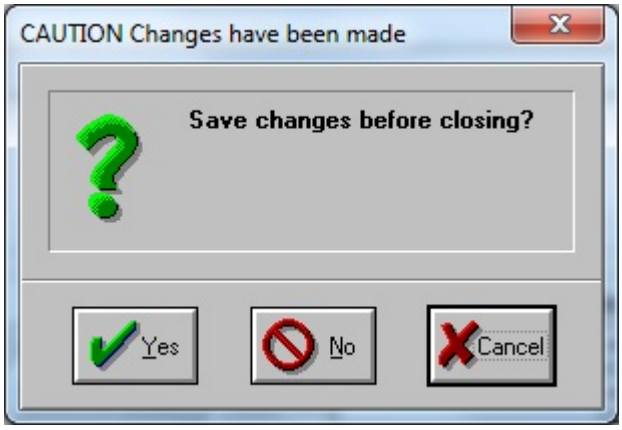
[Cut] Clicking this button copies the displayed point or area data to a clipboard and returns all values to their defaults.

[Copy] Clicking this button copies the displayed point or area data to a clipboard. Displayed values are not changed.

[Paste] Clicking this button copies the clipboard values to the displayed point or area data. The values on the clipboard are not changed and can be copied to more points or areas.

[Save] Clicking this button saves all changes to the database.

[Cancel] Clicking this button closes the dialog. If changes were made, the dialog below gives you another chance to save the changes by clicking the **[Yes]** button.



6.4.6 Alarm area setup

In the **Transponder Database** under the **File** menu, select the transponder where the alarm area is to be programmed in. Click the **[Edit Data]** button, followed by **Show areas** radio button and select the desired area.

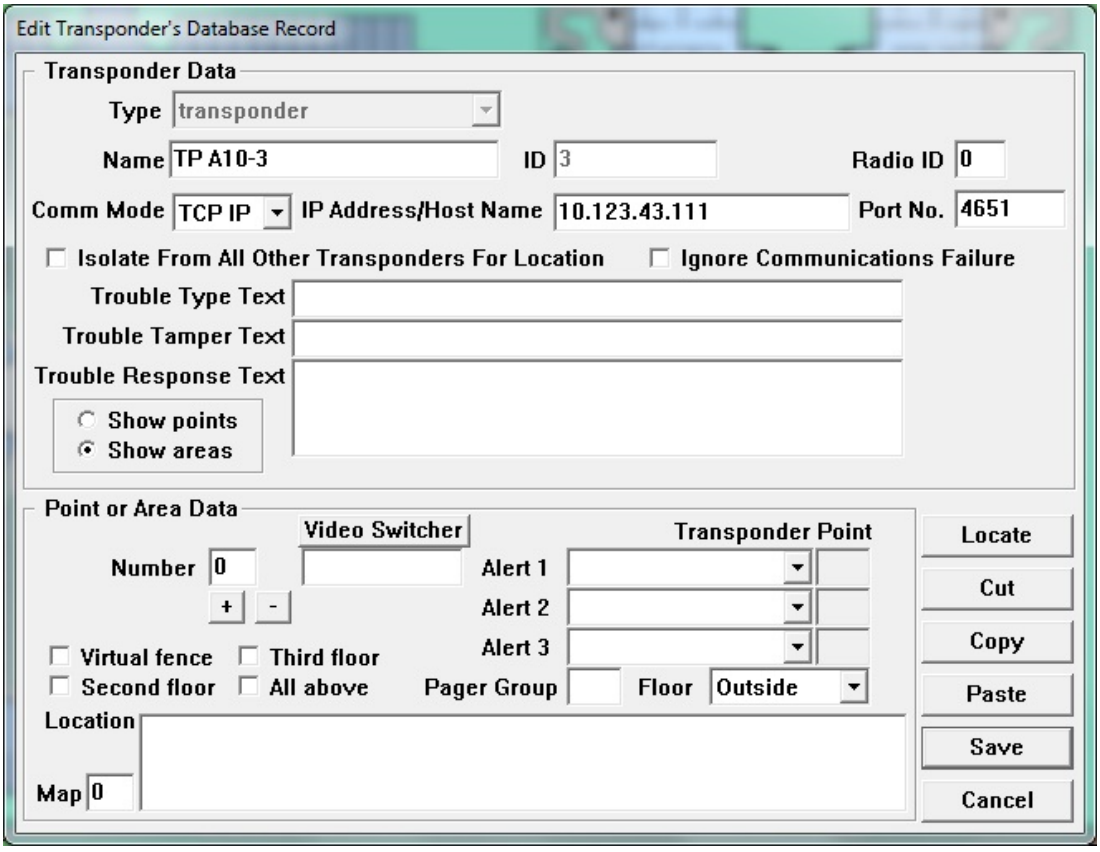


Figure 6.13: Transponder Area Edit Dialog

Number Each transponder can have up to 80 areas defined in them (prior to version 2.04 of the software, only 40 areas could be defined). This area number range from 0 to 79. Use the **[Locate]** button to define the area graphically on the map.

Video Switcher Selects a system serial port that is programmed in the **Remote Setup** dialog. The purpose is to display the area, where the alarm is most likely located, on the CCTV monitors near the Central Console. The string would activate a macro in the video switcher that selects the appropriate camera, and controls any required zoom and tilt actions. Up to 40 characters may be entered. Control characters may be entered as "^A" for control A.

Pager Group This **Pager Group** field may be programmed with a pager group that is paged if the alarm location is determined to be in this area. This pager group will be the first group paged to allow quick response by those individuals charged with responding to an alarm in this area. Each area may be assigned a pager group that can be the same or different from other alarm areas.
The default alarm **Pager group** defined in the **Pager Setup** dialog will also be paged after the pager group is assigned to an area. If a pager group is not assigned to an area or the alarm location is not within a defined area, then only the default pager group will be paged.

Floor Determines the floor number that this area is defined for. The areas on floors above and below this one may be defined differently. In order for an area to be selected when an alarm is received, the location determined by the Central Console must be located within the defined area, and it must be located on the designated floor.

Virtual Fence Area If this checkbox is checked, this area will not be used for normal alarm area location. This area will only be used to define a “Virtual” fence. Specific transmitters in the **Subscriber Database** can reference this transponder and area. When they reference this area, and the system locates the transmitter position outside the area, a wandering (“Virtual” fence) alarm will be generated. This alerts the operator and shows the position of the transmitter.

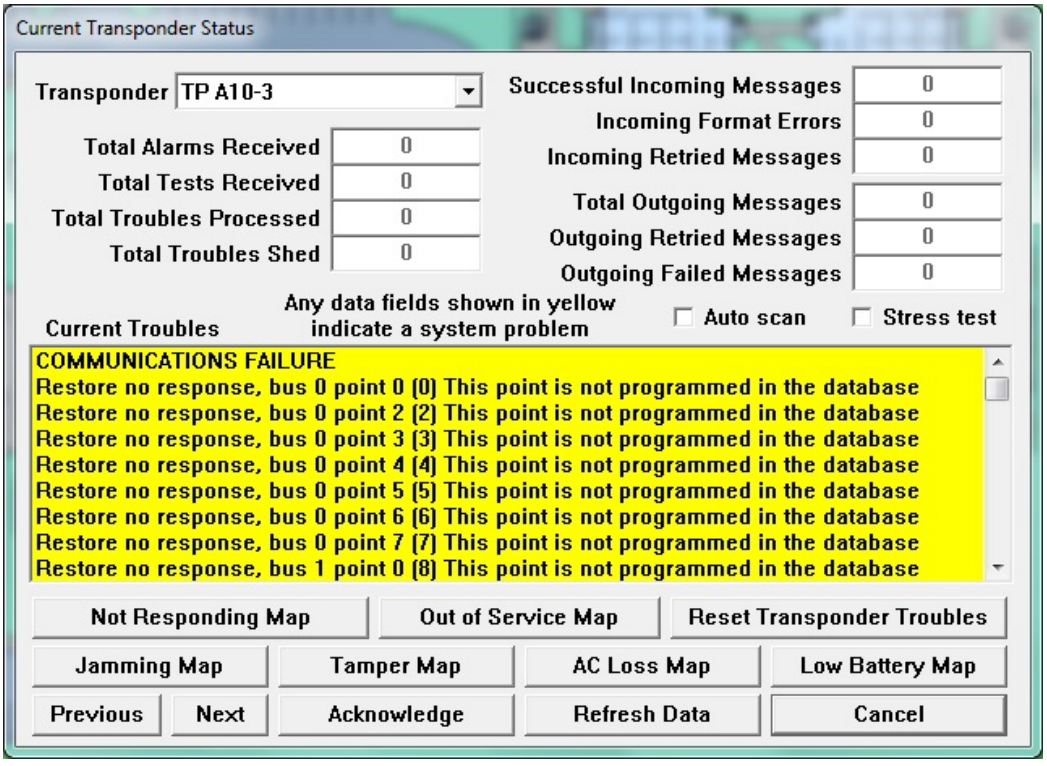
6.5 Powering up the system for the first time

After the system is configured, the system may be powered up. If the system uses multiple transponders, it is easier and more effective to power up the transponders one at a time. By doing this, troubleshooting time can be significantly reduced, especially for transponders to determine if there is a wiring problem in the SE485 bus between transponders.

Notice!

It is very important that twisted pair wiring is used for the SE485 bus. The Tx+ and Tx- wires must be twisted together and the Rx+ and Rx- wires must be twisted together.

1. Turn on the power switch on the first transponder. In the Security Escort Central Console software, select the menu **Setup > Transponder current status**. The following dialog window appears:

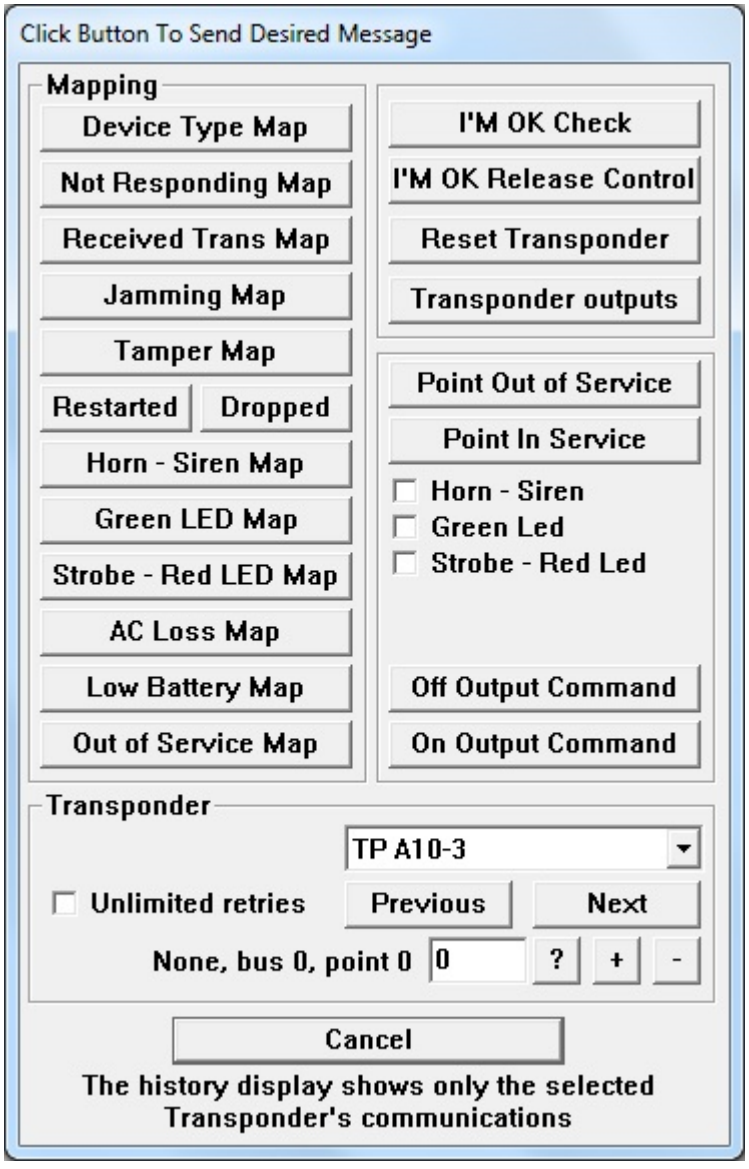

Current Transponder Status
Transponder TP A10-3
Successful Incoming Messages 0
Incoming Format Errors 0
Incoming Retried Messages 0
Total Alarms Received 0
Total Tests Received 0
Total Troubles Processed 0
Total Troubles Shed 0
Total Outgoing Messages 0
Outgoing Retried Messages 0
Outgoing Failed Messages 0
Current Troubles
Any data fields shown in yellow indicate a system problem
Auto scan
Stress test
COMMUNICATIONS FAILURE
Restore no response, bus 0 point 0 (0) This point is not programmed in the database
Restore no response, bus 0 point 2 (2) This point is not programmed in the database
Restore no response, bus 0 point 3 (3) This point is not programmed in the database
Restore no response, bus 0 point 4 (4) This point is not programmed in the database
Restore no response, bus 0 point 5 (5) This point is not programmed in the database
Restore no response, bus 0 point 6 (6) This point is not programmed in the database
Restore no response, bus 0 point 7 (7) This point is not programmed in the database
Restore no response, bus 1 point 0 (8) This point is not programmed in the database
Not Responding Map
Out of Service Map
Reset Transponder Troubles
Jamming Map
Tamper Map
AC Loss Map
Low Battery Map
Previous
Next
Acknowledge
Refresh Data
Cancel

2. Select the desired transponder. Click the **[Reset Transponder Troubles]** button. If the selected transponder is communicating with the Central Console, the number “1” will appear in the **Total Outgoing Messages** and **Successful Incoming Messages** fields. The transponder is now communicating with the Central Console software. If the number “1” only appeared in the **Total Outgoing Messages** field, there is a wiring problem between the Central Console and the transponder (refer to *Troubleshooting reference, page 100* of this manual and locate the problem).

3. Check the **Stress test** checkbox. This tests the communications reliability by causing the Central Console software to send a continuous stream of messages to the selected transponder. The values in the **Successful Incoming Messages** and **Total Outgoing Messages** fields should start counting up rapidly, with few if any errors. It is normal to have slightly fewer **Total Outgoing Messages** than **Successful Incoming Messages**. If the errors are greater than 1% of the number of messages, then there is a problem that should be corrected (refer to *Troubleshooting transponders, points, receivers, and alert units, page 95* of this manual and locate the problem).

4. After the stress test runs, any current troubles are displayed in the box in the **Transponder current status** window. Correct any troubles at this time.

5. From the **Setup** menu, select **Transponder communications**. The following dialog window appears:



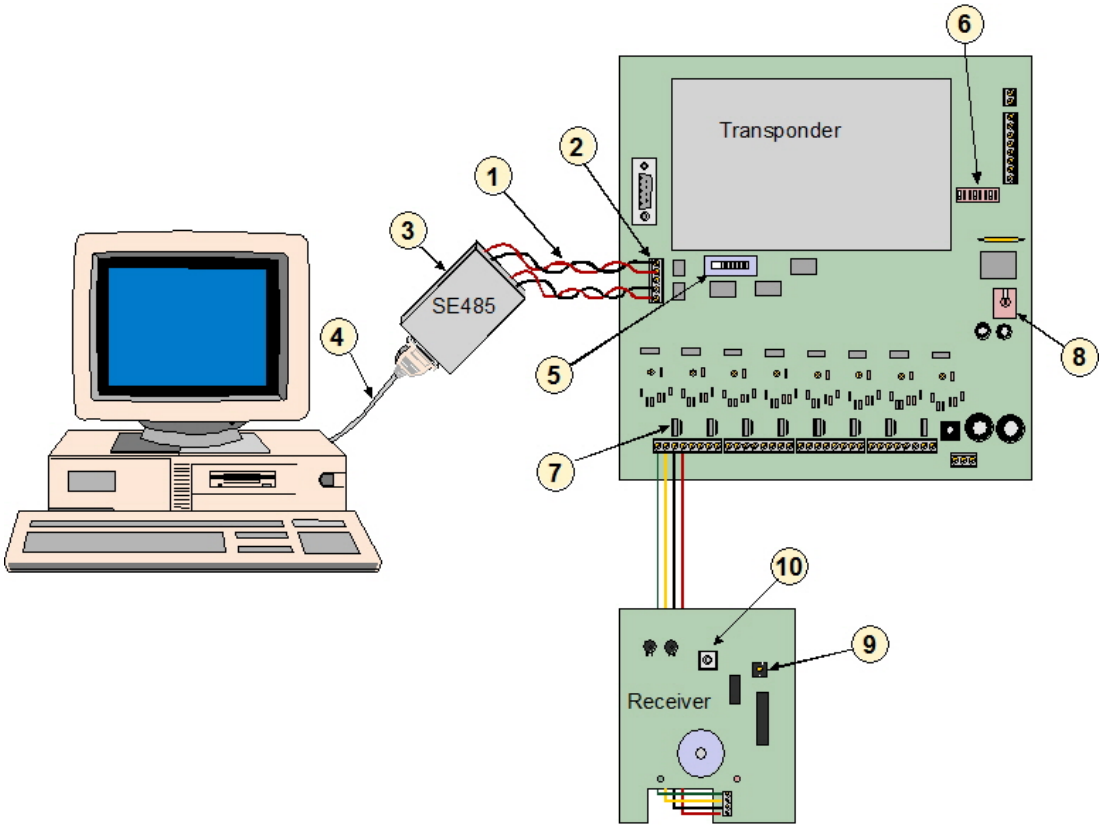
6. Select the desired transponder. Then click the **[Not Responding Map]** button. A grid should appear on the screen. The columns of the grid represent multiplex buses from 0 to 7 (left to right). The rows of the grid are points on the multiplex buses from 0 to 7 (bottom to top). At this point there will be a zero (0) on the grid location for each receiver connected to the selected transponder. A zero means that a receiver is programmed in the database and is communicating with the transponder. If the number 1 appears at a point location, the receiver is programmed in the database but not communicating to the transponder (refer to *Troubleshooting reference, page 100* of this manual and locate the problem). If an X appears on the grid at a point location the receiver is communicating to the transponder but is not programmed in the database. Reprogram this point in the database or rotate the receiver ID rotary switch on the receiver's circuit board to the proper point number. (Y = Alert unit is in the database but

not responding to the system; N = Alert unit is in the database and is responding to the system.)

7. When the transponder is communicating with all the receivers and the **Receivers Database** records are correct, back up the database files to the hard drive, if any changes were made. Select the menu **Utilities > Backup**, and make sure it is pointed to the hard drive. Click the **[Backup]** button. It is also wise to back up each database to a USB flash drive. Mark the USB flash drive label with the databases and backup date.

7 Troubleshooting transponders, points, receivers, and alert units

7.1 Common errors



1. Wrong type of cable. You must use twisted pair cable. Common errors are that twisted pairs are not used or separate wires from more than one pair is used.
2. Check to see if + and – are reversed or if TX and RX are reversed.
3. The correct connections from the SE485 to the transponder are: RX+ to TX+ and RX- to TX-.
4. The cable should be straight through to your computer serial port connector. Do not use a null modem cable or a cable marked for printer use.
5. Switch set in the wrong position.
6. DIP switch settings incorrect.
7. Power Jumper not on.
8. ON/OFF switch not ON.
9. Wrong point address.
10. Forgot to put on the tamper spring.

7.2 Built-in troubleshooting aids

7.2.1 Receiver

Jumpers

There are two groups of jumpers on the EA102A-304 receiver. The first group contains jumpers P1 through P3. The second contains jumpers P4 through P8. The function of each jumper is indicated in the table below:

Jumper	Operation with Jumper in Place
P1*	Sounder is enabled
P2*	Green LED is enabled
P3*	Red LED is enabled
P4**	Test mode is enabled
P5**	Receiver spacing mode is enabled
P6**	Left antenna is disabled
P7**	Right antenna is disabled
P8	Do not place a jumper across these pins

Notice!

* Remove jumpers P1, P2, and P3 when installed in an outdoor enclosure.

** Remove jumpers P4, P5, P6, and P7 for normal operation.

Test mode

Each EA102A receiver provides a test mode that may be used to check the unit's functionality. The module goes into test mode when jumper P4 is in place (jumper P5 removed). In this mode, all test and alarm receptions will be sounded.

Notice!

The sounder and LEDs (jumpers P1, P2, and P3) must also be enabled to operate the test mode.

Each receiver should be tested using the following method (test only one receiver at a time):

1. Enable the test mode by placing the jumper P4 across both pins (jumper P5 removed).
   - The red LED will turn ON and stay ON during the test. This indicates that power is properly connected and the receiver is in test mode. If the red LED does not come on check the POWER+ and POWER- wiring to this receiver. Also verify the corresponding transponder bus enable jumper is in place and the transponder is on and powered.
   - The green LED will flicker if the receiver is connected to a working transponder. If the green LED is not flickering verify the BUS+ and BUS – wiring to this receiver (note, this is a rapid flickering).
   - There will be no data transmitted to the Central Console. Therefore, the Central Console will report this receiver as "Not responding" while the receiver is in test mode.
2. Activate the transmitter from different locations near the receiver.
   - The red and green LEDs will respond to a received transmission.
   - If the receiver detected all the packets from the transmission, the sounder will beep three times.
   - If the receiver detected the transmission, but some of the packets were missing, it will beep once. This could indicate that the signal is not sufficient from this location.

3. Remove the jumper P4 to return the receiver to normal operating mode.

7.2.2 Transponder

Status LEDs

Each transponder contains LEDs that display the transponder's condition and its response to events. With the exception of the AC Power LED (which is located in the lower right corner of the transponder circuit board), the diagnostic LEDs are located in the top right corner of the transponder board.

Generally, the LEDs indicate the unit's status and signal system events. Each LED and its function is indicated below.

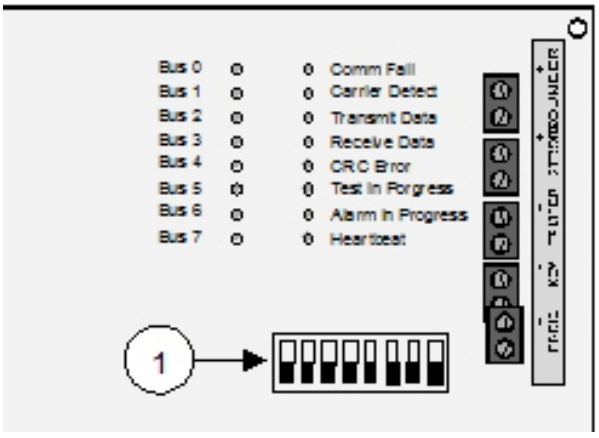


Figure 7.1: EA500 Diagnostic LEDs

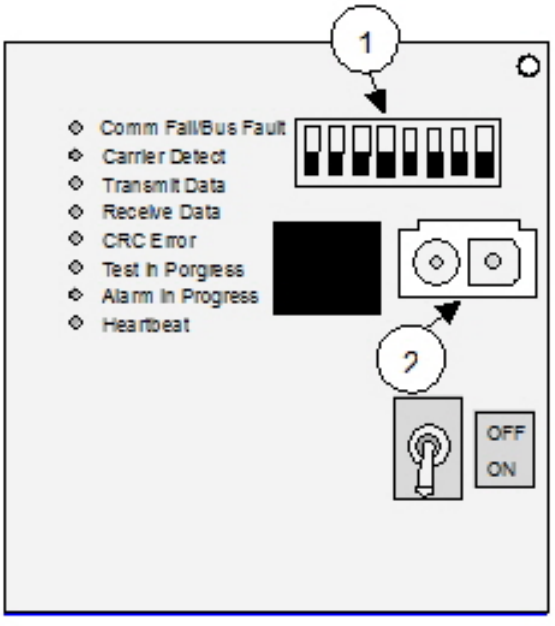


Figure 7.2: EA501 Diagnostics LEDs

LED	Function
AC Power	(Lower right corner of the transponder board.) If this LED is off there is no AC power (mains power) to the board. Find and correct the AC power (mains power) problem. This LED lights even if the transponder's power switch is off.
Comm Fail	This LED lights if the transponder is in a communications failure condition with the Central Console. It automatically goes out when communications are restored.
Carrier Detect	This LED is operational only for SE485 communications. It flashes every time any transponder (including this transponder) on this SE485 bus sends a message to the Central Console. It is used to monitor overall communications from the transponders to the Central Console. If the Carrier Detect LED stays on, there is a problem with one of the transponders on this bus, or the wiring, that must be corrected before normal communications are restored.
Transmit Data	This LED flashes every time this transponder sends a message to the Central Console, whether or not the Central Console receives it. If this transponder initiated the communications and the Central Console correctly receives the message, the Receive Data LED should flash soon after indicating the central station successfully returned an acknowledgement.
Receive Data	This LED flashes every time this transponder successfully receives a message addressed to it from the Central Console. If the Central Console initiated the communications, the Transmit Data LED should flash soon after indicating that this transponder is returning an acknowledgement.
CRC Error	This LED comes on every time a message is received containing errors, whether or not it was addressed to this transponder. The LED remains on until the next message addressed to this transponder is received without error. The most common cause for this LED to turn on is wiring errors. Verify that the SE485 TX+ and TX- are on a twisted pair. Also verify that the SE485 RX+ and RX - are on a twisted pair.
Test in Progress	This LED comes on whenever a transmitter is tested. It stays on for the duration of the test display, typically 5-sec. to 10-sec., then it goes out. If a test is received while another test is in progress, the Test in Progress LED goes out momentarily then comes on for the duration of the second test.

LED	Function
Alarm in Progress	This LED comes on whenever a transmitter is in alarm. It stays on for the duration of the transponder's involvement in the alarm, then it goes out. If an alarm is received while another alarm is in progress, the Alarm in Progress LED goes out momentarily then stays on as long as any alarms are active in the transponder. An alarm that causes the receiver sounders to stay on keeps the Alarm in Progress LED on. Silent alarms or alarms from unauthorized transmitters cause the Alarm in Progress LED to turn on and to go out when the Central Console acknowledges the alarm message. This also occurs for every alarm follower message. A maintenance alarm message causes the Alarm in Progress LED to come on for 5-sec. to 10-sec. then to automatically go off.
Heartbeat	Flashes at a fixed rate to indicate the microprocessor is operating normally. If this LED stops flashing, the transponder is not operational. Turn it off for 5-sec. using the power switch. Then turn it back on. If the LED does not flash, the transponder should have the AC power and the back-up battery disconnected. Wait a few seconds and then reconnect. If the LED does not flash at this time, the transponder should be replaced.
Bus 0 to 7	Normally these LEDs are on if the corresponding Bus Enable jumper is in place, and is off if the jumper is removed. If the bus is enabled, the LED flashes off and comes back on every time a receiver or alert module on that bus communicates with the transponder. A Bus LED flashes at the rate of the heartbeat LED if there is any kind of bus fault (data to ground, data to power, and bus power to ground) on that bus. On the EA501, the communications failure LED flashes at this rate since there is no Bus LED. A Bus LED flashes at half the rate of the Heartbeat LED if there are no points reporting on that bus (open connection). On the EA501 the communications failure LED flashes at this rate. If a Bus LED is flashing for a bus that is not enabled, it can be reset in the Central Console's **Transponder Data View** dialog by selecting this transponder and clicking the **[Clear EE]** button. There are two special displays on the Bus LEDs. All the Bus LEDs go out, and for 2-sec. a single LED is on. Walking down the display from bus 0 to bus 7 indicates that a battery test is in progress. Usually after the tamper switch is released, the bus LEDs count rapidly to indicate the EEPROM memory is being updated.

Verifying communications

To verify communications, press the test feature on any transmitter. The Test in Progress LED comes on. If it did not come on, the receivers are not communicating with the transponder. About a second after the Test in Progress LED comes on, the Transmit Data LED flashes (indicating the transponder is sending the test message to the Central Console). Less than a second later the Receive Data LED flashes (indicating the Central Console returned an acknowledgement).

Toggling the transponder's tamper switch on/off causes the Transmit Data LED to flash (indicating that the transponder is sending the tamper message to the Central Console). Less than a second later the Receive Data LED flashes (indicating the Central Console returns an acknowledgement).

7.3 Troubleshooting reference

7.3.1 Transponder communication with SE485 bus

Symptoms	Probable Cause	Possible Solutions
All transponders on one bus in communications failure	Power to SE485.	Check 9 V DC adapter for proper voltage. Red Power LED should be ON (on SE485).
	Wire between SE485 and transponder incorrectly installed.	Check to make sure transmit from transponder goes to receive of SE485 and receive from transponder goes to transmit on SE485 (RX+ to TX +, RX- to TX-).
	Open, short, or grounded cable from SE485 to first splice or transponder.	Use VOM to test cable for short, open or ground. Repair or replace cable. Also check for + - pair reversed.
	Wrong cable between SE485 and computer.	Cable should be a straight through cable to your computer serial port connection. Do not use null modem cable or cable marked for printer.
	Bad SE485 Module.	Replace SE485 Module.
	Using third party RS-485 interface.	Due to changes made for transient protection, transformer isolation, and link busy detection, these signals are not compatible with third party RS-485 Interfaces. Replace with SE485
High communications error count.	Wire between SE485 and transponder incorrectly installed.	Check to make sure transmit from transponder goes to receive of SE485 and receive from transponder goes to transmit on SE485 (RX+ to TX +, RX- to TX-).

Symptoms	Probable Cause	Possible Solutions
	Wrong wire type.	Wire type must be twisted pair.
Single transponder in communication failure.	Transponder not on.	Check power switch.
	Wrong transponder address.	Check DIP switch setting on transponder to correspond with your transponder data base setting.
	RS-232/SE485 switch position.	Check slide switch on transponder to make sure it is in the SE485 position.
	SE485 wiring on transponder.	Check to make sure transmit from transponder goes to receive of SE485 and receive from transponder goes to transmit on SE485 (RX+ to TX +, RX- to TX-).
	Close lightning hit.	Power down transponder and restart. If this does not work replace transponder.
	Bad transponder.	Replace transponder.

Table 7.1: Transponder communications with SE485 bus

7.3.2 Transponder communication with ProxLink

Symptoms	Probable Cause	Possible Solutions
Communication failures from all transponders.	Loss of power.	Check power to ProxLink from Central Console. Also, if using SE485, check power to SE485 module.
	Cable from ProxLink to computer.	Must use 25 to 9 pin cable supplied from Proxim.
	ProxLink Radio Module might be in Programming Mode.	Unplug power to ProxLink and plug back in to re-start ProxLink.
	SE485 Module.	Check wiring between SE485 and computer, and SE485 at ProxLink Radio Module. Transmit should be going to receive and receive should be going to transmit (RX+ to TX+, RX- to TX-).

Symptoms	Probable Cause	Possible Solutions
	Cable from SE485.	Cable from SE485 to computer must be straight through 25 pin to 25 pin or 25 pin to 9 pin depending on your serial port on the back of the computer. Do not use cable labeled for printer or null modem cable. Replace cable if bad. Check cable between SE485 and ProxLink Radio Module. Replace if bad.
	ProxLink Radio Module.	Check programming for Central Console ProxLink Radio Module to be sure it is correct. If everything else checks OK, replace ProxLink..
One transponder in communication fail on ProxLink Radio Module link.	Transponder.	1. Check slide switch on transponder to make sure it is in the RS-232 position. 2. Check DIP switch address for transponder to be sure it corresponds with **Transponder Database**.
	Cable from ProxLink Radio Module to transponder.	Replace cable.

Symptoms	Probable Cause	Possible Solutions
	ProxLink Radio Module.	3. Check power to ProxLink. Make sure radio power LED is lit. 4. Check antenna connection to ProxLink Radio Module. 5. Check programming for ProxLink Radio Module. 6. Radio out of range or not in line of sight of central console antenna. 7. Ice on antenna. 8. If antenna is remote from ProxLink, use RG8U cable to prevent dB loss. 9. Replace ProxLink Radio Module.
	SE485.	10. Check power to ProxLink to SE485. 11. Make sure slide switch on transponder is set for SE485. 12. Check wiring from transponder to SE485 (RX+ to TX+, RX- to TX-). Make sure transmit goes to receive and receive goes to transmit. 13. Replace SE485 Module.

Table 7.2: Transponder communication with ProxLink

7.3.3 Transponder communication with Moxa/Lantronix device

Symptoms	Probable Cause	Possible Solutions
Communication failures from all transponders.	Loss of power.	Check power to Moxa/ Lantronix device.
	Cable from Moxa device to transponder.	Must use standard 9 pin female to 9 pin male cable.
	Cable from Lantronix device to transponder.	Must use modified 25 pin male to 9 pin male cable. Refer to the Lantronix wiring notes.

Symptoms	Probable Cause	Possible Solutions
	Moxa/Lantronix device might not be running.	Unplug power to Moxa/ Lantronix device and plug back in to restart Moxa/ Lantronix device.
	Cable from Moxa/Lantronix device to Ethernet network.	Check Ethernet cable between Moxa/Lantronix device and Ethernet network. Replace if cable is bad.

Table 7.3: Transponder communication with Moxa/Lantronix device

7.3.4 EA500 transponder bus faults

Symptoms	Probable Cause	Possible Solutions\
Bus failure.	Bus power jumper not in place.	Place jumper on for corresponding bus (see the transponder's *Installation Instructions* for location of jumper).
	Short or open on the bus wires.	Put meter across bus wire. Should be reading between 7.5 V DC to 10.5 V DC. If voltage is not present or lower than 9 V, check wiring (BUS+ to BUS-) for possible ground, short, or open.
	No power to receiver.	Check power for 10.5 V DC to 13.5 V DC. If lower than 10 V DC or no voltage present, check wiring (PWR+ to PWR-) on power side of receiver, repair, or replace cable.

Symptoms	Probable Cause	Possible Solutions\
	Close lightning hit.	Power down transponder (AC and battery) for 30-sec., then turn power back on. If bus failure does not clear, probable cause would be bad bus on transponder.
	Bad bus on transponder.	Remove cable from bus, meter terminals with VOM. If voltage is lower then 9 V DC on BUS+ or lower then 12 V DC on PWR+, replace transponder.

Table 7.4: EA500 transponder bus faults

7.3.5 EA102 receiver issues

Symptoms	Probable Cause	Possible Solutions\
Single receiver not responding.	Address switch in wrong position.	Rotate switch to correspond with transponder database location.
	Open on the bus wires.	Put meter across bus wire. Should be reading between 7.5 V DC to 10.5 V DC. If voltage is not present or lower than 9 V, check wiring (BUS+ to BUS-) for possible ground or open.
	No power to receiver.	Check power for 10.5 V DC to 13.5 V DC. If lower than 10 V or no voltage present, check wiring (PWR+ to PWR-) on power side of receiver repair or replace cable.
	Defective receiver.	If power is present on BUS+ and PWR+ and rotary switch is set to correct address, replace receiver.
Single receiver intermittently not responding.	Receiver is located past the 900 m (3000 ft) maximum cable run.	Re-engineer location or reroute cable to be under 900 m (3000 ft).

Symptoms	Probable Cause	Possible Solutions\
	Moisture on circuit board.	Seal housing where moisture is entering enclosure. Replace receiver until the old one dries out.
	Cable going to ground occasionally.	Replace or repair cable.
	Insects nesting on circuit board.	Seal any entry point and spray insect repellent inside housing to stop any further invasions into receiver.
	Bad splice to receiver.	Check all splices to make sure cables are tight and not loose causing high resistant open.
	Defective receiver.	If power is present on BUS+ and PWR+, between 7.5 V DC and 10.5 V DC on bus, and 10.5 V DC and 13.5 V DC on power, replace receiver.
Single receiver reporting bad check sum.	Two receivers on the bus with the same address ID number.	Check rotary switches on all receivers on that bus to be sure there are no duplicate ID numbers.
	Moisture or water on receiver.	Replace receiver with new one until the old receiver dries out. Seal any point where moisture is entering the receiver housing.
	Length of cable to receiver. Receiver is mounted over 900 m (3000 ft.) from transponder.	Reconfigure the bus run to make sure receiver is within 900 m (3000 ft.) of the transponder.
	Bad splice to receiver.	Check all splices to make sure cables are tight and not loose causing high resistance open.
	Defective receiver.	If power is present on BUS+ and PWR+, between 7.5 VDC and 10.5 VDC on bus and 10.5 VDC and 13.5 VDC on power replace receiver.

Symptoms	Probable Cause	Possible Solutions\
Receiver jamming.	Electrical equipment in area causing jamming on receiver.	Go to the software dialog **Setup** r**eceiver configuration**. Increase jamming threshold by one degree at a time until jamming stops and receiver returns to normal. If jamming persists after increasing level, relocate receiver or attempt to identify and minimize the jamming source.
Receiver LEDs not working.	LEDs not positioned behind viewing lens.	Remove cover, straighten LEDs, replace cover carefully so LEDs are positioned behind viewing lens. Use maintenance transmitter on test and alarm after installing cover to check visibility of LED.
	Jumpers in “OFF” position on receiver.	Remove cover, check jumpers to right of sounder above red LED and make sure jumpers P2 and P3 are “ON”.
	Bad receiver.	After performing the steps above and LEDs still do not operate on test or alarm, replace the receiver.
Receiver’s sounder not operating.	Jumper in “OFF” position on receiver.	Remove the cover, check jumper to right of sounder above red LED and make sure jumper P1 is “ON”.
	“Run Silent” is turned on in the Central Console software.	At the Central Console, select menu **Setup** > **Transponder Parameter** dialog and un-check the **Run Silent** checkbox.
	Bad receiver.	If the sounder still does not operate after performing the steps above, replace the receiver.

Table 7.5: EA102 receiver issues

7.4 Receiver configuration dialog

Once the receiver and alert unit data for a transponder has been entered into the **Transponder Database**, this dialog is used to verify that each receiver is working and is properly addressed in the database. This setup tool identifies errors in the address switch settings of receivers and alert units as well as data entry errors in the **Transponder Database**.

To Confirm the RF Reception

To confirm the RF reception, LED, sounder operation and location of each receiver, select **Receiver configuration** from the **Setup** menu. The following dialog appears:

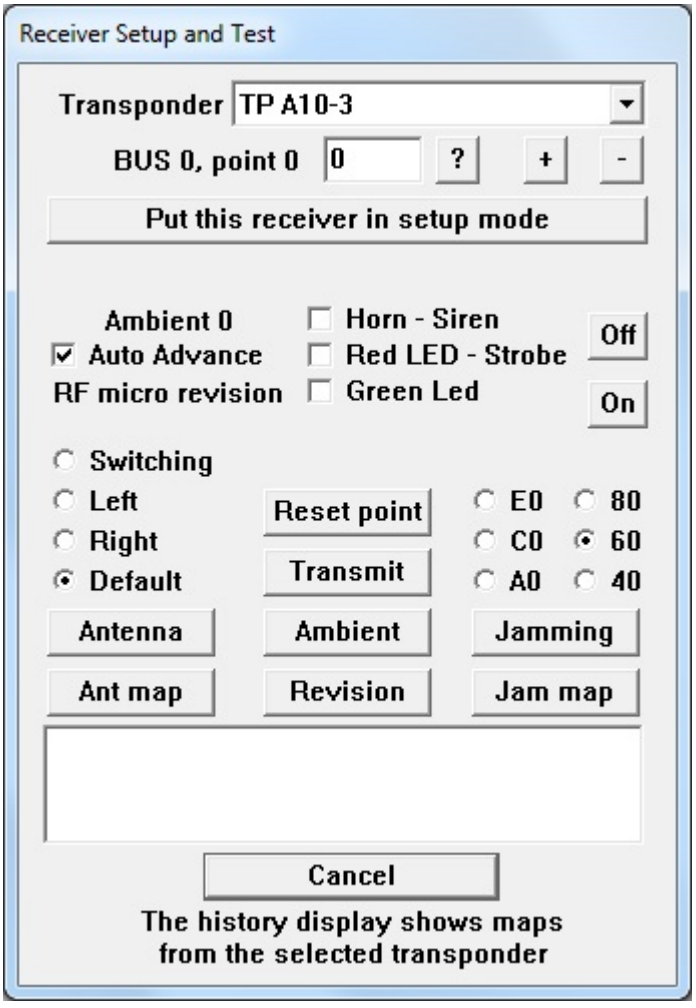


Figure 7.3: Receiver Configuration Dialog

Select the desired transponder. Click on the **[?]** button next to the point number. A bus and point grid will appear showing the programmed receivers. Click on the lowest point number button. If the first receiver is point 0, click on the **[0]** button, or if the first receiver is point 1, click on the **[1]** button. The point number will be automatically entered. Click the **[Put this receiver in setup mode]** button. The red and green LEDs will light for the selected receiver on the selected transponder.

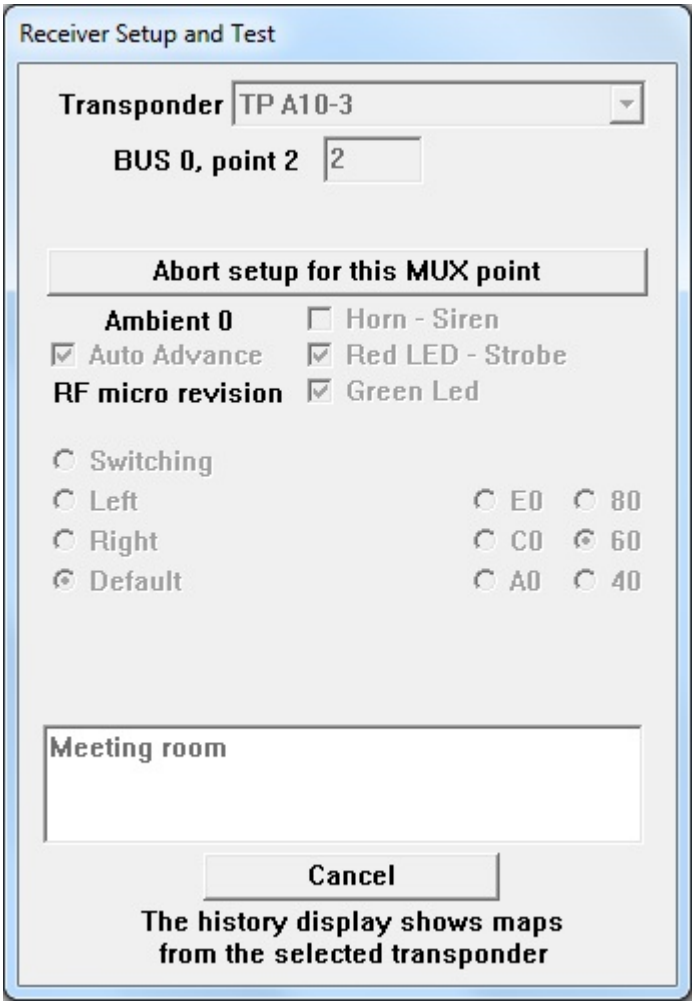


Figure 7.4: Receiver Configuration Dialog

Take the maintenance transmitter and go to the selected receiver. The red and green light should be lit up when you arrive at the first receiver location. Transmit an alarm from the maintenance transmitter. The receiver should activate by blinking the red lights and sounding the sounder (if the sounder jumper is in place on the receiver).
This will confirm that the RF portion of the receiver is working and you are at the right location. The software will then turn off the LEDs on the tested receiver. The receiver with the next higher point number will be automatically selected and its red and green LEDs will light. Proceed to that receiver and perform the same operation with an alarm on the maintenance transmitter until the operation of all receivers has been confirmed and all receivers are working and in their proper location on that transponder.
If the LEDs fail to light, the LED jumpers may be missing on that receiver, the receiver may be set to the wrong address, or you may be at the wrong location. If the LEDs are lit but the receiver fails to respond to the maintenance alarm, there may be a problem with the receiver board or another receiver is receiving the signal stronger.
Repeat the above sequence starting with step 1 for all transponders and receivers in the system.

Note: The illuminated LEDs indicate to the service person standing near the device that the receiver is actually the one currently in the setup mode. If the LEDs of the designated receiver are not illuminated, there is probably an error in the switch settings of the receiver or an error in the address in the **Transponder Database**. To help resolve such problems, the person at the Central Console can command any device to illuminate its LED's and/or sound its horn.

7.5 Post construction setup

7.5.1 Testing the location accuracy of an installation

Notice!
Before doing any of the following testing, it is important to verify that every receiver in the system is functioning correctly using the procedure described in the Security Escort *Hardware Installation Manual*. Additionally, every receiver must be programmed in the **Transponder Database** with its actual physical location and floor level. **It is also important that receivers that are physically stacked directly above one another on floors of a building are also located at the same X and Y coordinates in the database**.

There are three methods that can be used to verify the location accuracy of an installed system, using a standard subscriber transmitter or using a maintenance transmitter. Repeat the chosen process throughout all protected areas. Ask the customer for the areas where they have special concerns and devote extra attention to those areas, since the customer is likely to be more critical in those areas.
Remember the intent of the Security Escort system is to dispatch a responding individual to an area that will not add additional delay to their response to that duress call. Therefore, the computed location should be considered to be in error only when it would add unacceptable additional time to the alarm response.
While testing, it is helpful to see which receivers are involved in the alarm response and the relative reception level they reported. To display the receivers, select menu **Utilities** > **Security Preferences**. Make sure the **No receiver icons** checkbox is not checked and click the **[Save]** button. Select menu **Setup > System Preferences**. If **Show test levels** and **Show maintenance levels** checkboxes are checked, the relative reception level is shown in the receiver icons; otherwise, the floor number will be shown.
When testing with any of the following methods, the transmitter must be used exactly as it would be used in normal operation. A transmitter designed to be belt mounted or used in a holster must be in its normal mounting attitude and be worn on the belt of the individual originating the test transmissions. Handheld transmitters must be held in the hand about waist high, never held above the head.

Using a standard subscriber transmitter

1. This method requires two people with radio contact between them. One person operates the computer running the Security Escort software, and the other takes the subscriber transmitter to the area to be tested.
2. Press the alarm on the transmitter and remain at the spot where you transmitted.
3. The computer operator acknowledges the alarm and accurately describes the computed location over the radio. The individual with the transmitter should confirm the reported location or describe over the radio the actual location. Either individual must record all discrepancies, including the actual and computed locations.

We recommend using a map or floor plan and drawing an arrow from the actual alarm location to the reported location. It is also helpful if all successful alarm locations are marked with a **P** (passed), then the alarm can be reset from the computer screen.

4. For areas where there are alarm location problems, try facing in different directions in the same spot. Also generate additional alarms from different spots to fully understand the extent of the problem. You should generate alarms in areas adjacent to the area with the problem to see if they are also affected.

Using a maintenance transmitter with only one person

1. The Security Escort software retains the last 50 maintenance alarm locations. Make sure you are the only one using a maintenance transmitter on site, buddy check is off, and that you limit yourself to a maximum of 50 maintenance alarms per sequence.
2. Synchronize the time on your watch to the computer. Carry a detailed map or floor plan of the area to be tested that you can write on.
3. Take the maintenance transmitter to the area to be tested. Press the alarm on the transmitter and accurately mark the spot on the map where you transmitted with a “1” (for the first transmission). Also record the time of the first transmission only.
4. Continue to the next location, transmit and mark that spot on the map with a “2.” Repeat the process throughout the area to be tested, being sure not to exceed 50 alarm transmissions and making sure that at least 10-sec. elapse between transmissions.
5. When finished, return to the computer and select menu **File > Maintenance Alarm Database**. Scroll through the alarm list to find the alarm that matches the time of your first transmission. This is the maintenance alarm that you marked as “1” on your map.
6. Confirm that the actual location from the map matches the reported location.
7. If the actual location differs from the reported location, draw an arrow on the map from the actual location to the reported location. Press the up arrow once to go to the next alarm. Compare the locations, drawing an arrow to the reported location if they differ. Repeat this procedure for all points on your map, making sure that the points on the map stop when you run out of entries in the scrolling list on the computer screen. Otherwise, the points on the map and the screen are out of sync and the errors on your map are incorrect and misleading.
8. For areas where there were alarm location problems, you may want to repeat the process above facing different directions from the same spot. This generates additional alarms from different spots in the problem areas to fully understand the extent of the problem.
9. You should also generate alarms in areas adjacent to the area with the problem to see if they are also affected.

Using a maintenance transmitter with two people

1. The two people must have radio contact between them. One person operates the computer running the Security Escort software and the other takes the maintenance transmitter to the area to be tested.
2. At the computer select menu **File > Maintenance Alarm Database**. Make sure the top item in the scrolling list is selected.
3. Press the alarm on the transmitter and remain at the spot where you transmitted. At the computer, observe the alarm and accurately describe the computed location over the radio. The individual with the transmitter should confirm the reported location or describe the actual location over the radio. Either individual must record all

discrepancies, including the actual and computed locations. We recommend using a map or floor plan and drawing an arrow from the actual alarm location to the reported location. It is also helpful if all successful alarm locations are marked with a **P** (passed).

4. For areas where there are alarm location problems, try facing in different directions from the same spot.
5. Generate additional alarms from different spots to fully understand the extent of the problem.
6. You should generate alarms in areas adjacent to the area with the problem to see if they are also affected.

Reviewing potential problem areas

Review the potential problem areas on the maps with the customer to see which areas cause them concerns, and which areas they consider acceptable. If the customer considers an area acceptable, it is typically not worth spending additional time trying to improve the location accuracy in those areas.

7.5.2 Improving the location accuracy of an installation

Once we have identified those areas that must be improved, what are the options to improve the computed location accuracy?

Notice!

All changes using the following steps could potentially change the computed locations for all alarms at or around the changed area. Therefore, after any change is made, the entire vicinity around the changed area must be verified.

- Typically the first thought is to add more receivers in the problem area. Generally this is a bad approach. If the system was properly designed using the recommended grid layout, adding extra receivers in any area of the grid will distort the response in adjacent areas and floors. While it may seem to fix the problem area, typically it will create more problems in adjacent areas. The exception is when an area is shielded by something such as wire mesh in the walls that prevent the RF transmitted signal from passing through. Therefore, additional receivers may have to be added in the shielded area to ensure that all alarm transmissions will be heard.
- Verify that the location of the receivers in the **Transponder Database** is accurate to their physical location, and the receivers are indicated to be at the correct floor level. It is also important that receivers that were physically stacked directly above one another on floors of a building are also located at the same X and Y coordinates in the database.
- Try changing the **Transponder Database** location of receivers (not the actual physical location) one at a time while testing the alarm location response, using one of the testing methods above. For example, if alarms are getting pulled outside a building in one area, move the closest receiver (in the **Transponder Database**) to that area a little further into the building and retest. If the area can be corrected using this method, verify the surrounding areas to make sure they were not adversely affected. It is generally better if the correction is done in small steps while verifying the adjacent areas, rather than trying to correct the entire error in one step.
- Starting with version 2.03 and higher, the Security Escort software allows individual receiver sensitivity to be set in the **Transponder Database**. Receivers can be adjusted from 50% to 149% of their normal sensitivity. No physical receiver changes or upgrades are required. Try changing the **Transponder Database** sensitivity of receivers one at a

time while testing the alarm location response, using one of the testing methods above. For example if alarms are being pulled towards a particular receiver, lower its sensitivity in 10% increments and retest. If the area can be corrected using this method, verify the surrounding areas to make sure they have not been adversely affected. **It is generally better if the correction is done in small steps while verifying the adjacent areas, rather than trying to correct the entire error in one step**.

- Starting with version 2.03 and higher of the Security Escort software, there are five different location algorithms that can be selected on an individual receiver basis in the **Transponder Database**. “Classic” (original Security Escort algorithm), “Linear”, “Low“ pull, “Medium” pull and “Strong” pull. By default, when a receiver is set for outside or tunnel, it will use the “Linear” algorithm and all other receivers will use the “Low” pull algorithm. The receiver that hears the alarm transmission the strongest will determine the algorithm used for this alarm. Changing the **Transponder Database** algorithm setting for a receiver only affects the location when the alarm is close to this receiver and it hears the alarm the strongest. Change the **Transponder Database** algorithm setting for a receiver and test in its area, using one of the testing methods above. The stronger the pull the more the alarm will be pulled towards the receiver, with “Linear” having no extra pull. Verify the surrounding areas to make sure they have not been adversely affected.
- Starting with version 2.03 and higher of the Security Escort software, the five different location algorithms can individually limit how close other receivers must be to the level of the receiver hearing the alarm the best, before they will be included in the alarm. “Classic” (original Security Escort algorithm), “Linear”, “Low” pull, “Medium” pull and “Strong” pull each have a separate setting. By adjusting this setting you can control if distant receivers with low receive levels will be considered in the alarm calculation.
- Starting with version 2.03 and higher of the Security Escort software, you can add “Virtual” receivers in the **Transponder Database**. A “Virtual” receiver is added at one of the 64 points allowed per transponder. However, there is no physical hardware used. The “Virtual” receiver is intended to compensate in cases where there is a receiver imbalance. For example if a building with a dense population of receivers is adjacent to a fence with few receivers and an alarm occurs between them; the alarm location may pull towards the building. The “Virtual” receiver references to other physical receivers that must be on the same transponder. Only if both of the referenced receivers receive an alarm transmission, then the “Virtual” receiver will be added to the alarm as if was a physical receiver that heard the alarm at the average receive level of the two reference receivers.
  The “Virtual” receiver’s location and sensitivity may be adjusted the same as a physical receiver. After a “Virtual” receiver is added, verify the surrounding areas to make sure they have not been adversely affected. **In no event should a “Virtual” receiver be utilized as a cost savings measure to avoid the installation of an actual receiver**.

7.6 System preferences dialog

The **System preferences** dialog under the **Setup** menu contains a number of settings that govern the behavior of the Security Escort System.

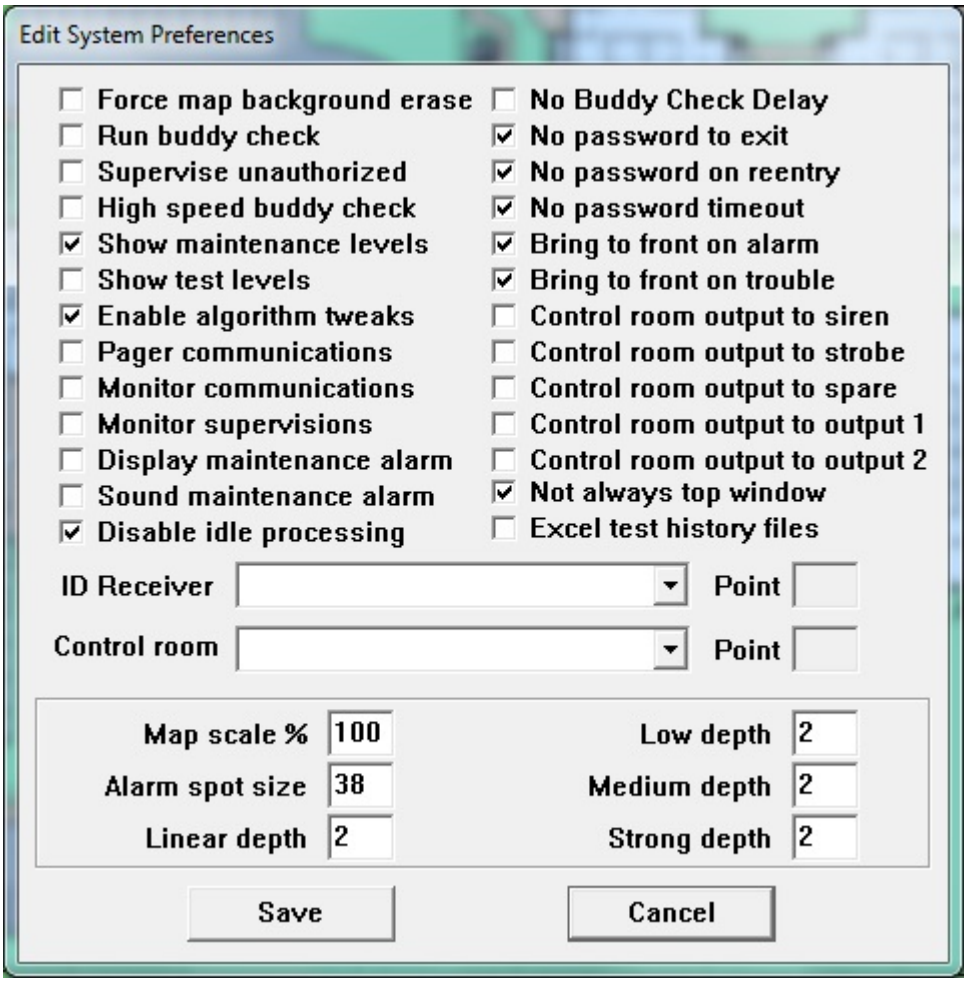


Figure 7.5: System Preferences Dialog

Force map background erase	Use this checkbox to erase the map screen. It should only be checked if there are problems with icons not being cleared properly from the screen. Otherwise it will cause the screen to flicker.
Run buddy check	This checkbox enables and disables the buddy check feature of the system. When checked, the Central Console periodically issues a command (via the transponders) to each receiver, to activate its on-board transmitter. The Central Console then compares the signals received from neighboring receivers to the results of earlier buddy checks, thus identifying receivers, which appear to have changed sensitivity.
Day month format	Checking this checkbox causes all dates to be presented in day month year format rather than the month day year format used in North America.
Supervise unauthorizedt	Supervise unauthorized transmitter.
High speed buddy check	Checking this checkbox allows the buddy check to run as fast as it can. Normally, only one buddy check transmission is sent each minute.

Show maintenance levels	Checking this checkbox causes the Central Console to display the signal strength measured by each receiver as a number (from 1 to 15) inside the receiver icon when maintenance alarms are displayed. Otherwise, the floor number is displayed.
Show test levels	Checking this checkbox causes signal strength levels to appear on the receiver icons when displaying tests on the main map screen. Otherwise the green test" icons are displayed.
Enable algorithm tweaks	Checking this checkbox causes the Map Scale, Alarm Spot Size, and depth settings to be displayed in this dialog. It also controls the display of the **SA%** and **Algorithm** settings in the **Edit Transponder's Database Record** dialog
Pager communications	Normally, this checkbox is not checked. If checked, the communications to the dial-up wide area paging system through the modem will be displayed on the history screen. This function is only used to diagnose communications problems to the paging system.
Monitor communications	Normally, this checkbox is not checked. If checked, the communications to the modem will be displayed on the history screen. This function is only used to diagnose communications problems with the modem.
Monitor supervisions	Monitor supervision alarms.
Display maintenance alarm	Normally, when a maintenance alarm is received from a maintenance transmitter, the red LED on all receivers hearing the transmission will flash for 5 seconds. If this checkbox is checked, the receiver with the loudest reception level will turn on both the red and green LED for 5 seconds.
Sound maintenance alarm	If this checkbox is checked, the receiver with the loudest reception level on a maintenance alarm will turn on its sounder for 5 seconds. Normally this checkbox is not checked.
Disable idle processing	Normally this software registers with Windows to return to the Security Escort System if there is any idle time. The Security Escort System can use it to speed up its response to serial communications and other background tasks. If checked, the software will not register for the idle time. Normally, this checkbox is not checked. Windows can show the amount of time each application (task) is taking. When this checkbox is not checked, it may appear that Security Escort System is "hogging" the processor resources. This is not true, because the Security Escort System is only taking the time that Windows gives it through the idle process. To prove this, check this checkbox. The amount of time that the Security Escort System needs will drop dramatically, and it will continue to operate normally (same communications responses will be slowed by several hundred milliseconds).
No buddy check delay	If checked, the software does not impose the hour between buddy checks from the same receiver. Normally, this checkbox is not checked and should not be checked for live systems.

No password to exit	If checked, the software will exit without asking for a password. Normally, this checkbox is not checked.
No password on reentry	If checked, the software will not ask for a password when the user switches to another program and then switches back to the still running Security Escort. Normally, this checkbox is not checked.
No password timeout	If checked, the software will not ask for a password after the screen saver kicks in. Normally, this checkbox is not checked.
Bring to front on alarm	If checked, the software will jump to the front when a new alarm occurs. Normally, this checkbox is checked.
Bring to front on trouble	If checked, the software will jump to the front when a trouble dialog pops up. Normally, this checkbox is checked.
Control room output to siren	If checked, whenever there is an unacknowledged alarm, the siren output on the control room output indicated below will operate.
Control room output to strobe	If checked, whenever there is an unacknowledged alarm, the strobe output on the control room output indicated below will operate.
Control room output to spare	If checked, whenever there is an unacknowledged alarm, the spare output on the control room output indicated below will operate.
Not always top window	If the Security Escort System is intended to be the only application running on this computer, leave this checkbox unchecked. This will prevent other applications from taking over the screen. The Security Escort System will always be present. If the Security Escort System is to be run on a computer with other applications, check this checkbox and it will share the computer's display like all other Windows applications. After checking this checkbox, stop and restart the Security Escort System for this feature to take effect. This checkbox is unchecked by default.
Excel test history files	**Do not check this checkbox in a live Security Escort System.** It is for diagnostic Engineering testing only.

ID Receiver / Point

Assign a receiver for automated transmitter exchanges. The Security Escort System contains a feature where the transmitter identification number can be automatically entered into the **Subscriber Database**. This is used for entering transmitters when first issuing them to subscribers and for transmitter exchanges.
This automatic capture of the transmitter identification number is accomplished by performing certain procedural steps (see the Security Escort *Operation Manual*) and then using the transmitter to make a test transmission in close proximity to a designated receiver, usually located close to the Central Console. By capturing the transmitter identification number in this manner, keystroke errors are avoided during database entries and changes. The receiver chosen for this purpose is designated as the **ID Capture Receiver**. To assign the **ID Capture Receiver**, its transponder name and its **Point Number** are selected using the boxes labeled **ID Receiver** and **Point**.

Control room / Point

The Security Escort System Software can activate an output to attract attention when there is an alarm that has been received and no operator has responded to the system yet. To assign the control room output, select the transponder it is connected to, and its **Point Number**.

Map scale %

This value changes the scale that the maps are presented with. It is not intended for normal operation, but is typically used for testing to allow more of the map to be seen. The setting may range from 30% to 400%. The **Enable Algorithm Tweaks** checkbox must be checked for this to be displayed.

Alarm spot size

This setting changes the size of the yellow dot that marks the calculated location of the alarm. The settings range from 19 to 76 (half to double the default alarm dot size). It is best to set the size of the alarm spot so that represents a diameter of 15.24 m (50 ft.) on the displayed map, as this is the area where the transmission of the alarm most likely took place. The **Enable Algorithm Tweaks** checkbox must be checked for this to be displayed.

Linear depth

This setting controls the involvement of receivers in the alarm location calculation only when the “Linear Algorithm” is being used. The setting can range from 0 to 6 (default is 2). When set to 0, only the receivers closer to the actual location of the alarm will be considered in the location calculation. As the setting is raised, more distant receivers will be included in the alarm calculation. Typically, lower settings are better than higher settings. This setting should be changed if there are known problems with the location using the “Linear Algorithm”. The **Enable Algorithm Tweaks** checkbox must be checked for this to be displayed.

Low depth	This setting controls the involvement of receivers in the alarm location calculation only when the “Low Algorithm” is being used. The setting can range from 0 to 6 (default is 2). When set to 0, only the receivers closer to the actual location of the alarm will be considered in the location calculation. As the setting is raised, more distant receivers will be included in the alarm calculation. Typically, lower settings are better than higher settings. Change this setting if there are known problems with the location using the “Low Algorithm”. The **Enable Algorithm Tweaks** checkbox must be checked for this to be displayed.
Medium depth	This setting controls the involvement of receivers in the alarm location calculation only when the “Medium Algorithm” is being used. The setting can range from 0 to 6 (default is 2). When set to 0, only the receivers closer to the actual location of the alarm will be considered in the location calculation. As the setting is raised, more distant receivers will be included in the alarm calculation. Typically, lower settings are better than higher settings. Change this setting if there are known problems with the location using the “Medium Algorithm”. The **Enable Algorithm Tweaks** checckbox must be checked for this to be displayed.
Strong depth	This setting controls the involvement of receivers in the alarm location calculation only when the “Strong Algorithm” is being used. The setting can range from 0 to 6 (default is 2). When set to 0, only the receivers closer to the actual location of the alarm will be considered in the location calculation. As the setting is raised, more distant receivers will be included in the alarm calculation. Typically, lower settings are better than higher settings. Change this setting if there are known problems with the location using the “Strong Algorithm”. The **Enable Algorithm Tweaks** checkbox must be checked for this to be displayed.
Alarm zone	Four alarm zones allow the selection of which alarms from specific transmitters are reported on this workstation. This workstation displays the alarms only for the alarm zones that are checked. Each transmitter can be assigned to one or more alarm zones and when that transmitter generates an alarm (if this workstation has one or more of the same alarm zones checked), that alarm is displayed. The system defaults to all alarms displayed on all workstations.
[Save]	Save the changes and close the dialog window.
[Cancel]	Cancel the changes and close the dialog window.

7.7 Security Preferences dialog

The **Security Preferences** dialog is used to make important settings that govern how the Security Escort System reacts in the event of alarm and test transmissions from the subscribers’ transmitters. This dialog is available only to the Security Director or his/her key operator.

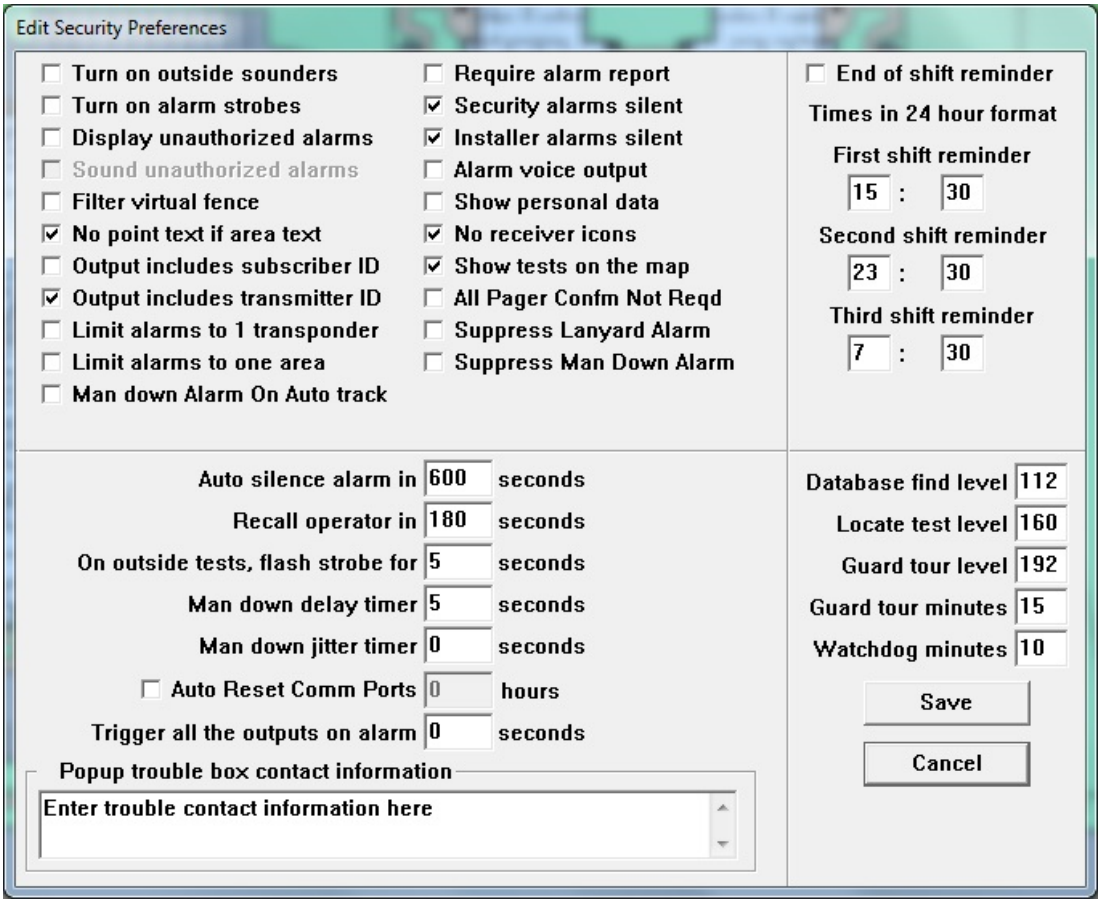

Edit Security Preferences
Turn on outside sounders
Turn on alarm strobes
Display unauthorized alarms
Sound unauthorized alarms
Filter virtual fence
No point text if area text
Output includes subscriber ID
Output includes transmitter ID
Limit alarms to 1 transponder
Limit alarms to one area
Man down Alarm On Auto track
Require alarm report
Security alarms silent
Installer alarms silent
Alarm voice output
Show personal data
No receiver icons
Show tests on the map
All Pager Confm Not Reqd
Suppress Lanyard Alarm
Suppress Man Down Alarm
End of shift reminder
Times in 24 hour format
First shift reminder
15 : 30
Second shift reminder
23 : 30
Third shift reminder
7 : 30
Auto silence alarm in 600 seconds
Recall operator in 180 seconds
On outside tests, flash strobe for 5 seconds
Man down delay timer 5 seconds
Man down jitter timer 0 seconds
Auto Reset Comm Ports 0 hours
Trigger all the outputs on alarm 0 seconds
Popup trouble box contact information
Enter trouble contact information here
Database find level 112
Locate test level 160
Guard tour level 192
Guard tour minutes 15
Watchdog minutes 10
Save
Cancel

Figure 7.6: Security Preferences Dialog

Most of the options given are simple checkboxes. To activate or deactivate the option given, click on the checkbox adjacent to the text. A check mark appears in the checkbox adjacent to activated option, empty checkboxes signify deactivated options. Some options in the **Security Preferences** dialog require numerical values. To change the current values, click the text box containing the values, then type in a new value.
Clicking the **[Save]** button saves the modifications and exits the **Security Preferences** dialog. Click the **[Cancel]** button to save the changes made so far, to discard the changes, or to remain in the **Security Preferences** dialog.

Turn on outside sounders This checkbox is used to activate or deactivate the sirens on alert units and transponders. Some security directors prefer that all alarms be silent, others choose to employ sirens. Checking this option causes the sirens on the alert units, to sound in the event of an alarm. Temporarily deactivating the sounders may be necessary during maintenance.

Turn on alarm strobes Checking this option causes the strobe lights on the alert units and transponders, to flash in the event of an alarm.

Display unauthorized alarms	This checkbox determines if “unauthorized" alarms are to be displayed on the Central Console. Unauthorized alarms are those triggered by transmitters not currently registered in the **Subscriber Database**. These could be transmitters that have been removed from the database because they were lost or stolen, they could be transmitters not yet issued, or they could be transmitters issued to subscribers at another Security Escort System. Typically this checkbox should not be checked.
Sound unauthorized alarms	This checkbox determines if "unauthorized” alarms are to be sounded on the horns of the receivers and the sirens of the alert units and transponders. The option is not available unless the **Display unauthorized alarms** option is selected. Typically this checkbox should not be checked.
Filter virtual fence	If the virtual fence option is be used, this box may be checked if some false alarms are generated to reduce the number of the false alarms. If it is checked then the actual alarms will be delayed by the supervision period of the transmitter.
No point text if area text	This checkbox affects the location text shown on the alarm screen. If this checkbox is checked and the alarm is determined to be within a predefined area then only the area text will be displayed (any receiver location text will be suppressed). Typically this checkbox should be checked.
Output includes subscriber ID	If this checkbox is checked, then any time the system prints or displays text for an alarm or test the subscriber’s ID number will also be displayed. Otherwise the subscriber’s ID will not be shown.
Output includes transmitter ID	If this checkbox is checked, then any time the system prints or displays text for an alarm or test the transmitter ID number will also be displayed. Otherwise the transmitter ID will not be shown. Typically this checkbox would not be checked.
Limit alarms to 1 transponder	This checkbox should not be checked. It was used only in a system where all transponders operate on areas that are separate from each other. It would prevent all interactions between receivers on different transponders. Typically this would be very undesirable and there is now a selection on an individual transponder basis to accomplish this feature.
Limit alarms to one area	This checkbox should not be checked. It is used only in a system where all transponders operate on areas that are separate from each other.
Man down Alarm On Auto track	If this checkbox is checked, then any time there is a man down alarm, the auto track functionality will be activated. Otherwise there is no auto track functionality for the alarm.

Require alarm report	If this checkbox is checked, the operator will be prompted to complete an alarm report when the alarm is reset from the screen. If the responding officer is required to complete the report, or if no system report is desired, this box should not be checked. If the operator should complete the report then check this box.
Security alarms silent	If this checkbox is checked, then alarms transmitted by security or watchman transmitters are to be silent, alerting the operator at the Central Console, but not sounding the sirens of the alert units or the horns in the receivers.
Installer alarms silent	If this checkbox is checked, then alarms transmitted by transmitters issued to installing company representatives and visitors are to be silent, alerting the operator at the Central Console, but not sounding the sirens of the alert units or the horns in the receivers. Typically this checkbox would be checked.
Alarm voice output	If this checkbox is checked, then predefined sound (.WAV) files can be played at the alarm console for specific alarm types. Typically this checkbox would not be checked.
Show personal data	If this checkbox is checked, then personal height, build, hair and eye color data will be displayed on the alarm screen.
No receiver icons	If this checkbox is checked, then individual receiver icons will not be shown on the alarm map display. Typically this checkbox would be checked.
Show tests on the map	If this checkbox is checked, tests from subscriber's transmitter will be displayed on the normal map screen as **OK** or **FAIL** icons, signifying a successful test by a valid subscriber or an attempted test transmission from a transmitter not in the **Subscriber Database**. This option doesn't affect the display the subscriber receives from a receiver or alert unit's strobe. Typically this checkbox would be checked.
All Pager Confm Not Reqd	If this checkbox is checked, the confirmation pager message is not sent to the any of the pagers when the alarm is acknowledged by an acknowledgement transmitter.
Suppress Lanyard Alarm	If this checkbox is checked, the lanyard alarm is suppressed and not reported.
Suppress Man Down Alarm	If this checkbox is checked, the man down alarm is suppressed and not reported.
Auto silence alarm in 'X' seconds	This box determines the length of time that the sirens and horns will sound before being automatically silenced by the Central Console. When the sounders are automatically silenced in this way, the Central Console remains in its alarm mode. The numerical value is in seconds, and it can be set between 0 and 9999. Typically this value would be set to prevent violating local noise ordinances and it defaults to 240 seconds (4 minutes).

Recall operator in 'X' seconds	This box determines the length of time before a recall alert is issued to the operator at the Central Console when an alarm is being displayed. If neither the mouse nor any key has been actuated for the specified length of time, the Central Console will trigger the alarm sound once. This feature prevents inadvertently ignoring an active alarm event. The numerical value is in seconds, and it can be set between 0 and 240. Typically this would be set to 60 seconds.
On outside tests, flash strobe for 'X' seconds	The entry in this box controls the approximate length of time the strobe on an alert unit will flash to signify a successful transmitter test. The value is in seconds, and can be set between 0 and 15. Typically it is set to 5 seconds.
Man down delay timer 'X' seconds	This value controls the time that a transmitter must be in a man down condition before a man down alarm is displayed. Typically it would be set to 10 seconds. Setting this value too short will cause inadvertent man down alarms to be generated.
Man down jitter timer 'X' seconds	This value controls the time that a transmitter will not be considering any man down alarm if man down alarm is received immediately after restore and before jitter time expire. This setting will not be used in normal system.
Auto Reset Comm Ports 'X' hours	This value controls the time that all the comm ports in the system will be automatically reset after configured duration. This setting is used only if any communication failure is observed and should not be used unnecessarily.
Trigger all the outputs on alarm 'X' seconds	This option turns on all outputs of the transponders, and alert units for the duration configured (1-255 seconds) when alarm is generated. If someone acknowledges an alarm during this duration, all these outputs will be turned off. Otherwise, after this duration has lapsed, all these outputs will be turned off automatically. If this value is set to 0, the system will trigger the outputs during alarms in the default normal behavior.
End of shift reminder	A check in this checkbox causes a prompt to appear on the Central Console screen every 5 minutes for 30 minutes prior to the end of each shift if there are incident reports that have not yet been completed. It is intended for responding officers to complete alarm reports before the end of their shift.
First, Second, Third shift reminder	The entries in these fields are the times (24-hour clock) at which the Central Console will prompt the operator that there is one or more incident reports that have not yet been completed. Prompts will be given only if the **End of Shift Reminder** option is selected.
Database find level	This is the minimum receive level (1-255) that must be heard before the system will automatically enter the transmitter in the **Subscriber Locate** dialog. It determines the distance the subscriber's transmitter must be within the specified ID capture receiver (set in the **System Preferences** dialog) before the system will recognize the test.

Locate test level	This is the minimum receive level (1-255) that must be heard before the system will accept a test generated by a transmitter other than a guard, to be printed with a location. It determines the distance the transmitter must be within from a receiver before the system will recognize the test and print the location. If the transmitter is too far away from the receiver, that receiver's green light will not be displayed, so the guard knows that they must move closer to the receiver for the test to register.
Guard tour level	This is the minimum receive level (1-255) that must be heard before the system will accept a test generated by the guard's transmitter to be entered as a location in the guard tour report. It determines the distance the guard's transmitter must be within from a receiver before the system will recognize the test and create the guard tour entry. If the guard is too far away from the receiver, that receiver's green light will not be displayed, so the guard knows that they must move closer to the receiver for the test to register.
Guard tour minutes	This setting controls the time spacing, in minutes, for entries of the guard's current location in the automatically generated guard tour report. Therefore if set to 15 minutes, an entry will be generated each 15 minutes that the guard's transmitter is within range of the system.
Watchdog minutes	This setting controls the time spacing, in minutes, for entries of the guard's current location in the automatically generated guard tour report. Therefore if set to 15 minutes, an entry will be generated each 15 minutes that the guard's transmitter is within range of the system.
Popup trouble box contact information"	Each yellow, pop-up trouble box that is displayed on the Central Console advises of system problems, containing specific instructions for the operator. Entries in this text box will be displayed in the pop-up trouble boxes whenever a system problem occurs that requires attention. This information usually includes the name and telephone number of the designated Security Escort maintenance technicians.

7.8 System Defaults dialog

This dialog allows the names for each class of subscribers to be changed to match the specific application of this Security Escort System.

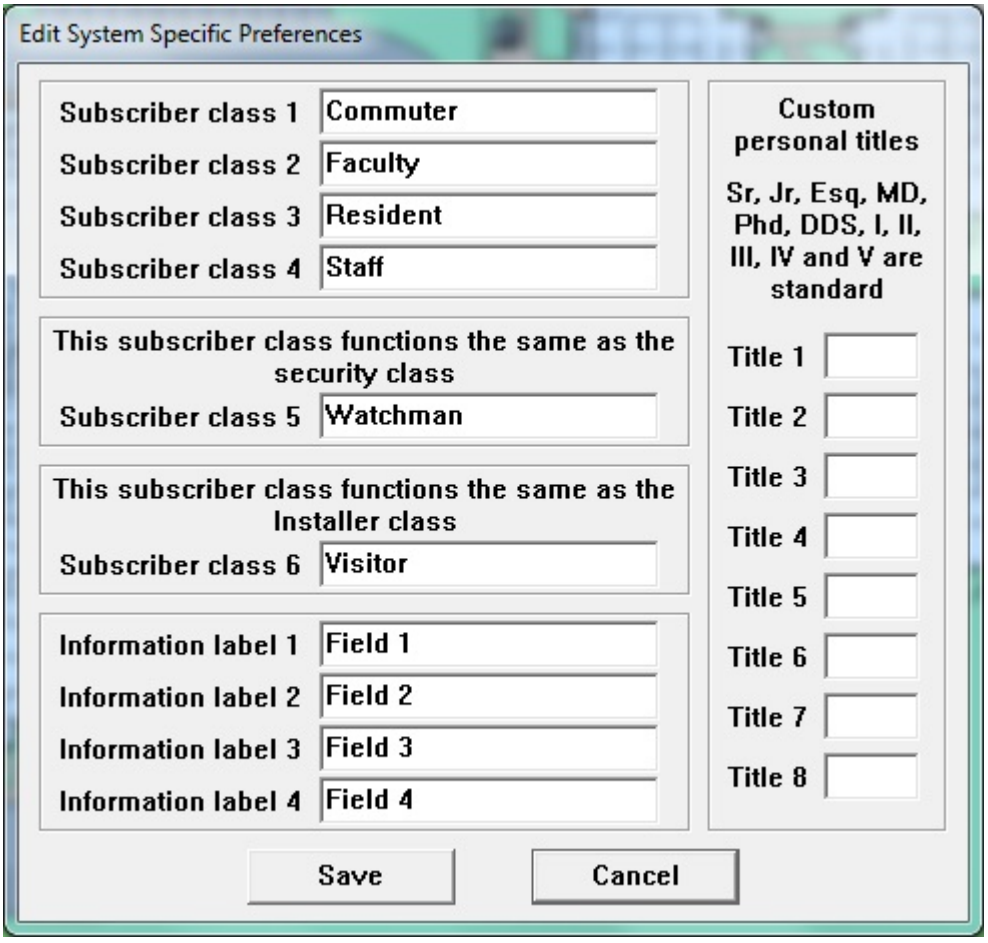


Figure 7.7: System Defaults Dialog

Titles that are entered into the **Subscriber Name** field in the **Subscriber Database** are entered here. The system alphabetizes the **Subscriber Database** entries by last name. When a title is entered after the last name, the entry is alphabetized incorrectly by title. Entering the titles prevents this problem.
The labels for the four **Information label** in the **Subscriber Database** are also changeable here.

7.9 System Labels dialog

The alarm type definitions are customized to customer’s requirements in this dialog window.

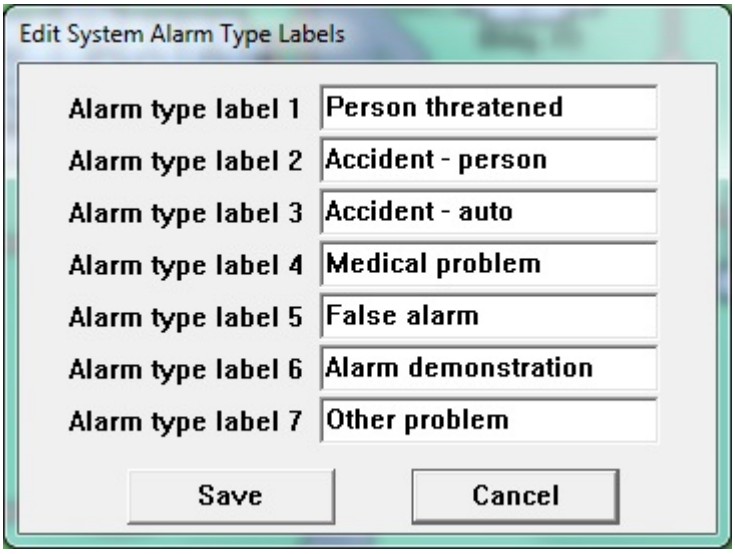


Figure 7.8: System Label Dialog

7.10 Subscriber Database

A subscriber is anyone who has been issued a Security Escort transmitter. This database includes all transmitters assigned in the system, whether they are protecting people or things. The **Subscriber Database** is very similar to the **Operator Database**; the method by which the names and other information are stored is virtually identical.

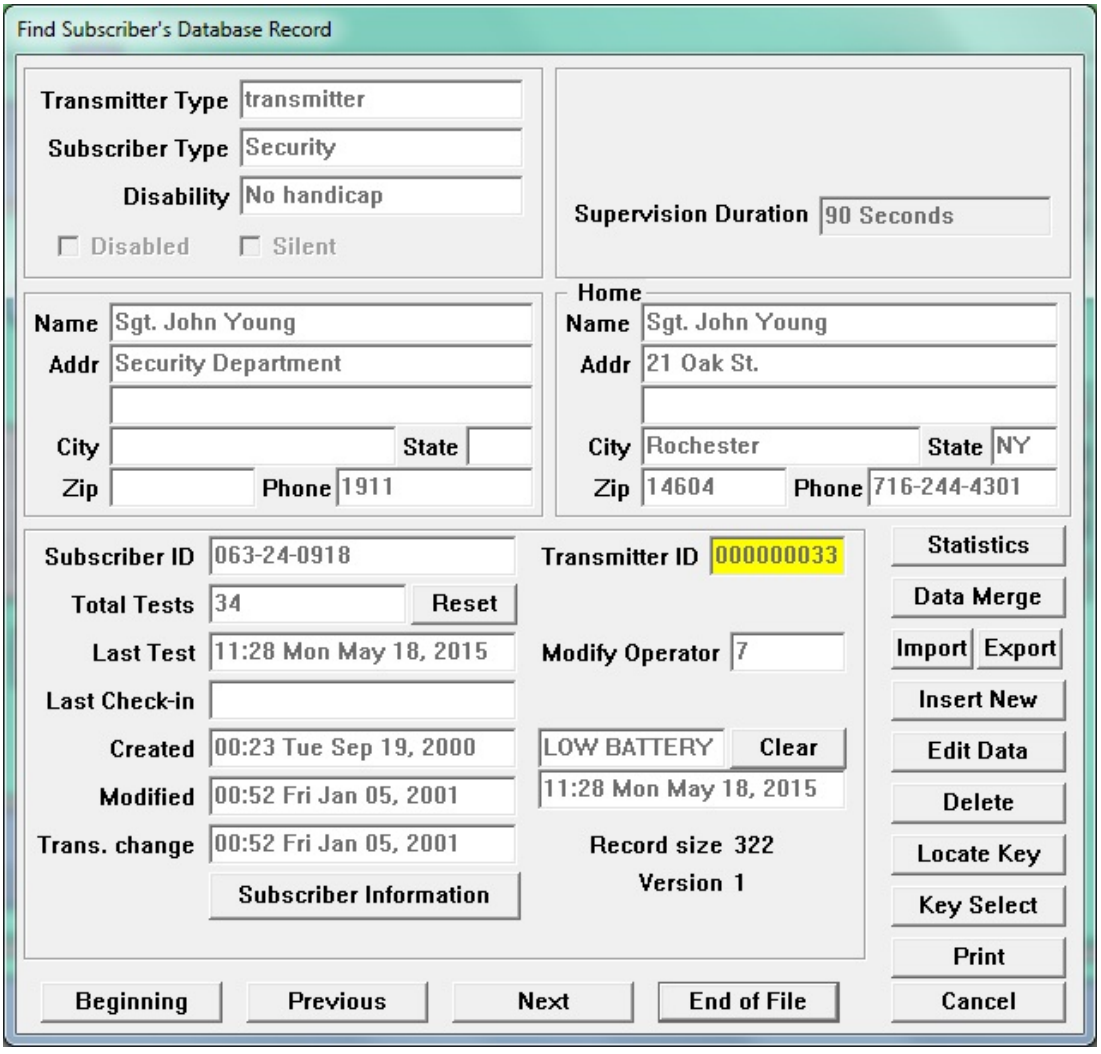


Figure 7.9: Find Subscriber's Database Record

The information stored in a subscriber's file includes the person's name, local address and phone number, permanent address and phone number, subscriber identification number (typically the individual's Social Security number), the transmitter identification code (each transmitter has its own unique code which identifies the subscriber during tests and alarms), and the subscriber's classification (commuter, resident, faculty, staff, and so on).

[Reset] Clicking the **[Reset]** button clears the number of **Total Tests** count.

[Clear] Clicking the **[Clear]** button removes the **Low Battery** indication. This should only be done after the transmitter battery is replaced or a new transmitter is issued.

[Print] Clicking the **[Print]** button displays the **Subscriber Print** dialog.

7.10.1 Print Subscriber Database

Clicking the **[Print]** button displays the **Subscriber Print** dialog. Select one of the indicated sort orders and the data fields that you desire in the report.

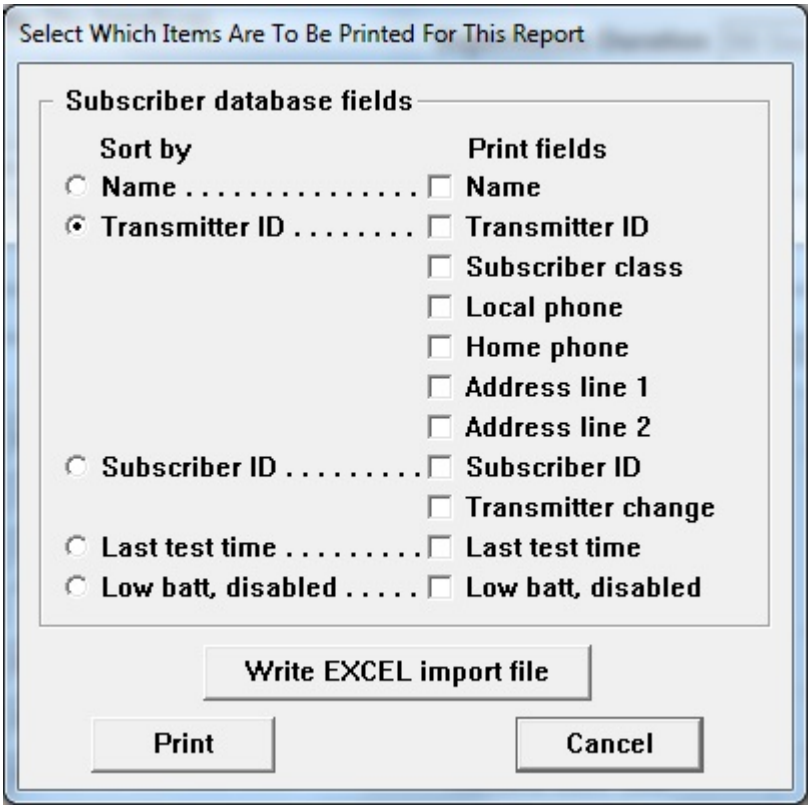

Select Which Items Are To Be Printed For This Report
Subscriber database fields
Sort by
Print fields
Name . . . . . Name
Transmitter ID . . . . . Transmitter ID
Subscriber class
Local phone
Home phone
Address line 1
Address line 2
Subscriber ID . . . . . Subscriber ID
Transmitter change
Last test time . . . . . Last test time
Low batt, disabled . . . . . Low batt, disabled
Write EXCEL import file
Print
Cancel

Figure 7.10: Subscriber Print Dialog

[Write EXCEL import file]	Clicking the **[Write EXCEL import file]** button causes all the fields of all the records to be sent to the “subscrib.txt” file in the folder in which Security Escort was installed. This file may be directly imported into Microsoft Excel or any other application that accepts tab delimited text..
[Print]	Clicking the **[Print]** button causes the selected data fields to print on the report printer in the indicated sort order.
[Cancel]	Clicking the **[Cancel]** button aborts the print dialog and returns to the previous screen.

7.10.2 Edit Subscriber Database record

When editing a subscriber’s file or creating a new file, the following information must be entered to complete the file: subscriber name, subscriber identification number, and transmitter identification code. The computer does not allow the edit screen to be closed until all of the mandatory fields are completed. The accuracy of information in the **Subscriber Database** is very important: in the event that a subscriber transmits an alarm, the information displayed in the alarm screen is taken from this database. A faulty address could hinder security’s response to an alarm.

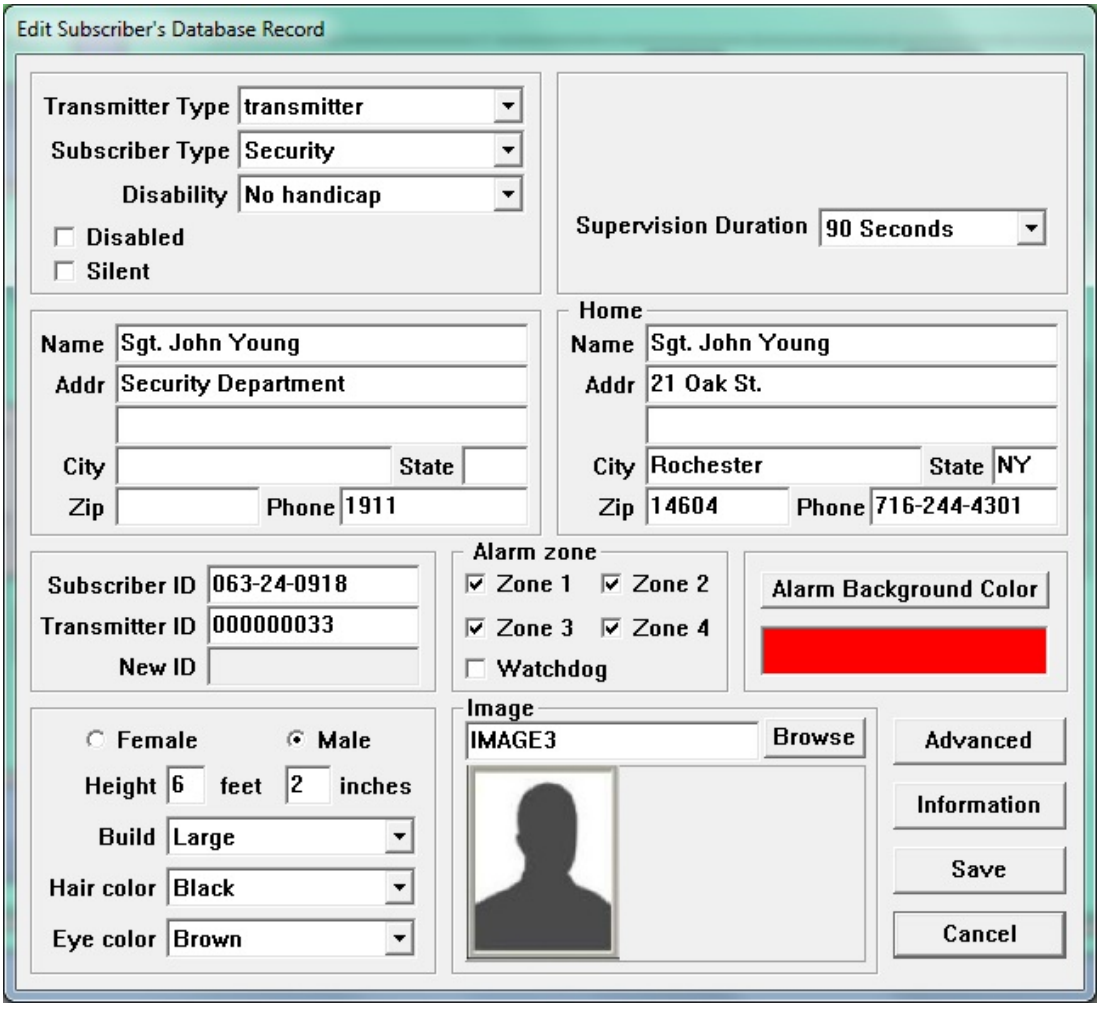


Figure 7.11: Edit Subscriber's Database Record (Transmitter)

Transmitter Type	Click the drop-down list to select the type of transmitter that is assigned to the subscriber. Currently, only the standard transmitter is supported.
Subscriber Type	Click the drop-down list select the appropriate class for this subscriber or asset. Selecting the subscriber type allows the alarm signal to be used to acknowledge alarms remotely. It does not create an alarm. When this transmitter transmits an alarm, the alarms present on the alarm screen are acknowledged in the order they were received. This is the same order the alarms would be received on a pager for a approving officer. The **Subscriber Type** available: Acknowledgement – subscriber with acknowledgement transmitters Commuter – normal subscriber type Faculty – normal subscriber type Installer – subscriber with maintenance transmitters Out of Service – out of service transmitters Point type – point transmitter for monitoring assets Resident – normal subscriber type Security – subscriber with security transmitters Staff – normal subscriber type Unclassified (default) Visitor – normal subscriber type Watchman – normal subscriber type
Disability	If this individual is handicapped, select an item from this drop down list. The condition is displayed on the alarm screen. If a handicap is selected, the **Notes** field will not show on the alarm screen.
Disabled	There is an option to disable an individual subscriber's transmitter in such a way that it does not produce an alarm message on the Central Console. This can be used to halt a subscriber’s misuse of the system. Disabling or enabling a subscriber is accomplished by locating the subscriber in the **Subscriber Database**, clicking on the **[Edit Data]** button, and clicking the checkbox next to **Disabled** in the upper-left corner of the dialog. If the box has a check mark, the subscriber's transmitter is ignored by the system; if it does not, the transmitter is recognized and alarms are displayed.
Silent	If checked, a system that normally sounds alarms is silent for all alarms generated by this transmitter.

Supervision Duration	Specific transmitter types periodically transmit supervisory messages so the system can monitor their function and location. The supervisory feature must be enabled in the transmitter. For transmitters with the supervisory feature enabled, select the interval for these Supervisory messages from the drop-down list. The values for the drop-down list are “None”, “10 Seconds”, “30 Seconds”, “90 Seconds” and “1 Hour”. The supervision period specific to the assigned transmitter must be selected if this feature is used.
Name	The individual or item assigned to this transmitter. This is a required field.
Address	Address of this individual or item within the protected area. The first address line on the left side, which is not the home address, is shown on the alarm screen.
City	City of this individual or item within the protected area.
State	State of this individual or item within the protected area.
Zip	Zip code of this individual or item within the protected area.
Phone	The phone number to access this individual within the protected area. The phone number on the left side, which is not the home phone, is shown on the alarm screen.
Subscriber ID	The **Subscriber ID** (typically the Social Security Number) must be typed into this field. This is a required field. It must be filled in with a unique ID.
Transmitter ID / New ID	The transmitter identification code can be typed into this field, but a much faster and error free method is to delete any existing entry in the **Transmitter ID** field and then perform a test with the transmitter to be assigned to this subscriber. The new **Transmitter ID** displays in the **New ID** field. The new **Transmitter ID** must be manually entered into the **Transmitter ID** field, or use the mouse to highlight the existing **Transmitter ID** and press and hold the <Shift> key and press the <Insert> key. (This transfers the new **Transmitter ID** to the correct field.) This is a required field; it must be filled in with a unique ID. Complete the change to the Subscriber information by clicking the **[Save]** button.
Alarm Zone	Specific alarm zones are assigned to the different computer workstations of the Security Escort system. Each transmitter entered in the **Subscriber Database** can be assigned to one or more of the alarm zones. You may control on which computer workstations alarms from this transmitter appear.
Alarm Background Color	Select the desired background color to display for alarm when this transmitter is activated.
Female/Male **Height** **Build** **Hair color** **Eye color**	These characteristics are shown on the alarm screen.

Image / [Browse]	Enter the filename for the image of this individual or item to be shown on the alarm screen. Click the **[Browse]** button to open a dialog box to select the filename from a list of available files.
[Advanced]	Used to set up special transmitters that monitor fixed locations. These features are not used for personal transmitters. This button is available only to the maintenance and installation personnel (see the Security Escort *Technical Reference Manual*).
[Information]	The **[Information]** button is used to enter specific information about the holder of this transmitter.
[Save]	Clicking the **[Save]** button saves all changes to the database.
[Cancel]	Clicking the [**Cancel]** button allows you to abort and cancel all changes to the database. A confirmation dialog box appears asking for confirmation to save changes before closing. Click the **[Yes]** button to save the changes, **[No]** button to abort the changes, or **[Cancel]** button to return to the **Edit Subscriber** dialog.

7.10.3 Additional subscriber information

The **[Information]** button is used to enter specific information about the holder of this transmitter. Car type, parking sticker number, license number, and medical information are examples of the types of information typically entered. Each field typically holds different information. The installer can change the field labels to labels that would define your intended usage.

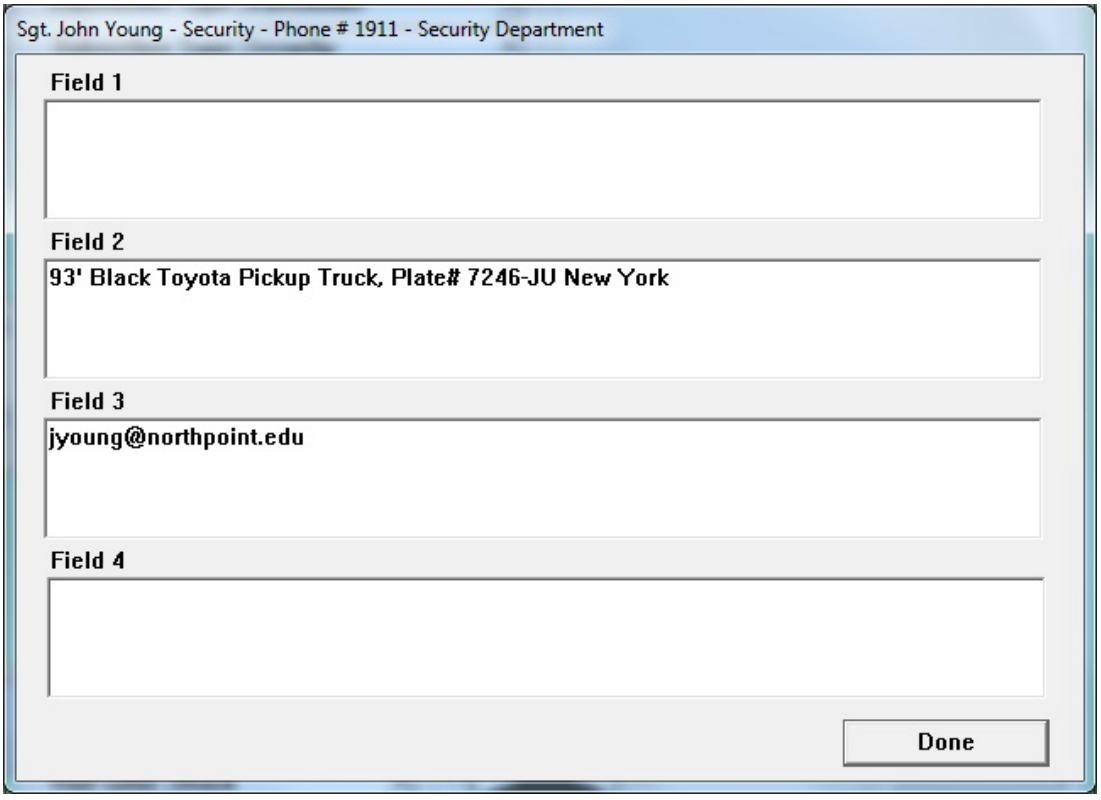


Figure 7.12: Information Entry Screen

[Done] Clicking the **[Done]** button closes the information entry dialog and returns to the **Edit Subscriber's Database Record** dialog. Clicking the **[Save]** button saves all changes to the database.

7.10.4 Subscriber images

This software does not capture the images, it displays images that were previously captured by some other means. The subscriber image can be captured using a digital camera, video capture board etc. The source of the image is not critical. We have not identified, nor require a specific manufacturer of the image capture equipment. The images must be saved individually in JPG format. The images should not be larger that 160 pixels wide and 160 pixels high. If they are they will have to be scaled and therefore they may loose image quality. The path to the images is set in **Subscriber image file path** field (default location of the images is "C:\ESCORT\IMAGES", but they can be located anywhere) found in the menu **Network > System directories and network address** dialog. The three-character file extension of the image files is set in **Extension** field (default is "JPG"). Subscriber images may also be saved in Windows bitmap (.BMP). However this format requires significantly more disk storage.
Only when the display is set to 640 x 480 (not recommended), the images are displayed on top of the map and the **Scaling %** field (10 to 200) controls the size of the image (try different settings to control the image size in the alarm screen). From the menu **Files > Subscriber Database** dialog, select the desired subscriber, then click the **[Edit data]** button. The **Image** field is the name of file of this subscriber's image. For example, if the subscriber's image is stored in a file with the name "Image1.jpg", enter "Image1" in this textbox.

You should have a minimum of a 1 MB video card memory to display the subscriber's images. To get the best color displayed on your LCD monitor, make sure to set it to "True Color (32-bit)". Open Screen Resolution by clicking the Start button Picture of the Start button, clicking Control Panel, and then, under Appearance and Personalization, clicking Adjust screen resolution. Click Advanced settings, and then click the Monitor tab. Under Colors, select True Color (32 bit), and then click OK.
(256 color likely will produce undesirable results). When in doubt set to High Color. In the same dialog "Desktop area" can be set to 640x480, 800x600 or 1024x768 pixels. When the display is set to 640x480 (not recommended) the images are displayed on top of the map and therefore limit how much of the map displayed. The 1024x768 setting may require too much memory for most video cards and show more of the map, decreasing the size of the map details. Most video cards can be set to 800x600 and when in doubt this setting should be selected. If you can't choose these settings you video card or monitor setting may be incorrect, refer to the system documentation to correct.

7.10.5 Fixed Location Transmitters

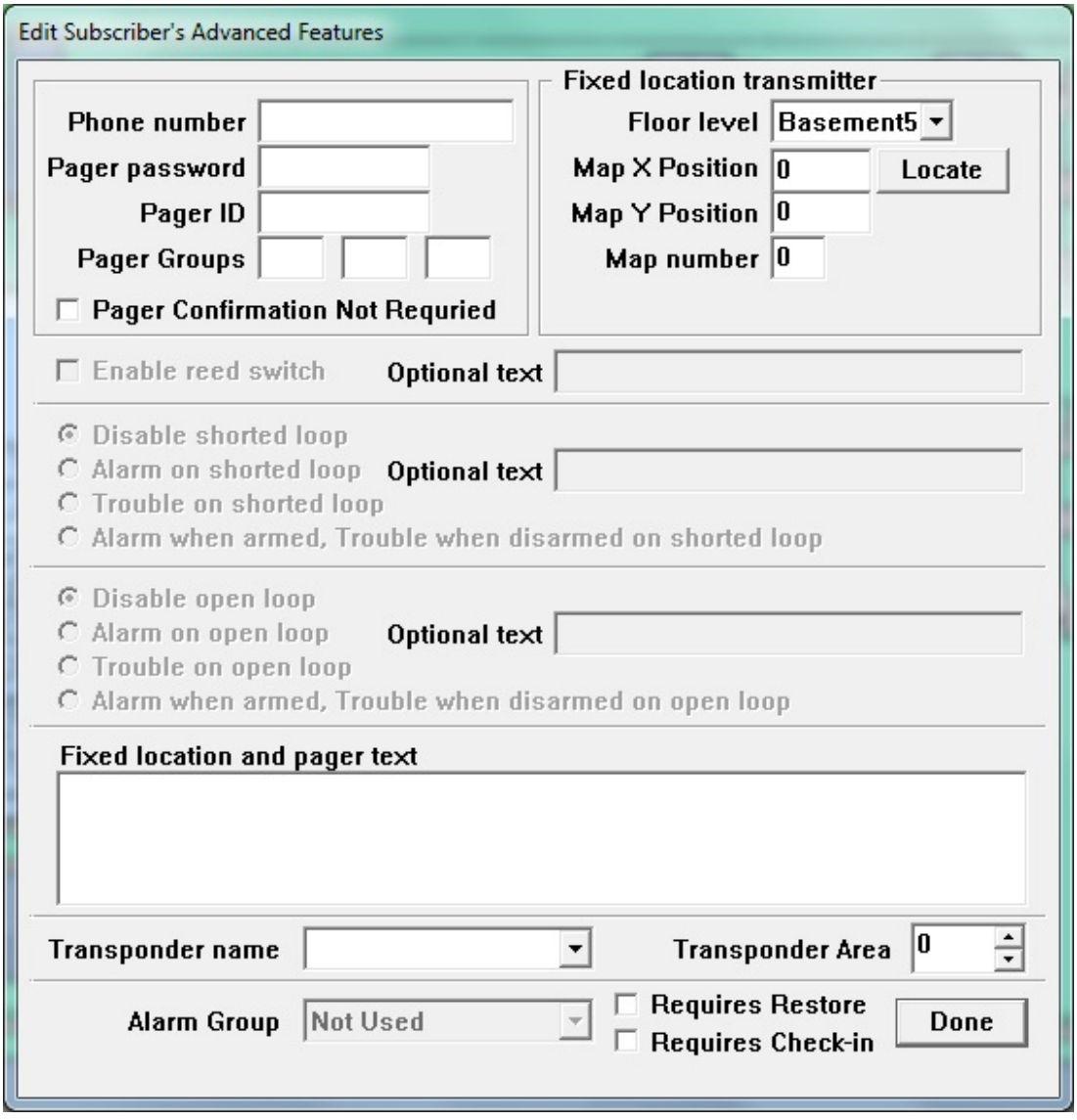


Figure 7.13: Fixed Location Dialog

Different paging companies and they may require different baud rates. Set the baud rate to the highest baud rate common to all of the paging companies to be accessed.
The Character limit (characters per page), Pages per call affect all pages of the indicated type (local and dial-up). These fields must be set to the lowest setting for any of the routes that may be used. Remember that dial-up pages may be routed to different paging companies and they may have different restrictions.

7.10.6 Subscriber (individual) Pager Setup

In the **Subscriber Database** select the record for the desired individual. Click the **[Edit Data]** button, followed by the **[Advanced]** button. The dialog below will be displayed.

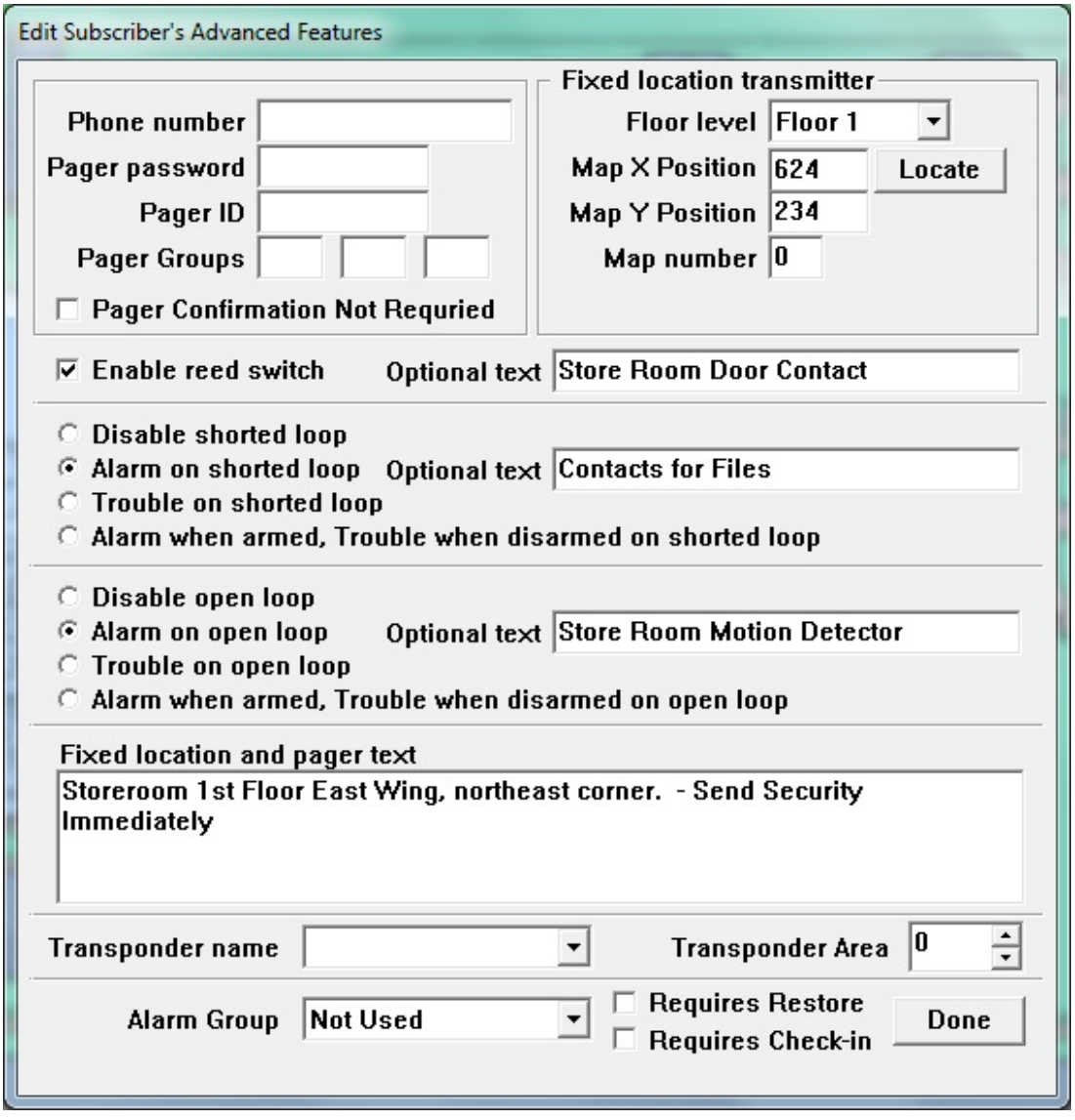


Figure 7.14: Subscriber Database Advanced Dialog

The pager ID is required for all individual pagers dial-up and local. If the phone number and password are assigned the page will be sent over the modem connection. If the phone number and password fields are blank the page will be routed to the local paging system. If you do not desire this individual to have pager support leave the phone number, password and pager ID fields all blank.

If the pager information is entered above this individual may be assigned to 3 paging groups. Each group will accept 8 members maximum. Remember it takes time to communicate with a paging service, therefore only add members to a group if they need to be there, otherwise you may slow the paging report to people that must respond.

A pager group may contain members accessed by the local paging system and members that require dial-up access. Dial-up access typically takes much longer and it may slow pages to the local paging system.

7.10.7 Subscriber Database Advanced Features

The **Subscriber Database** contains the information on the transmitters that are assigned in the system. See the Security Escort *Operation Manual* for the basic operations of the **Subscriber Database** dialog. See the section on *Exporting, importing and merging the Subscriber Database, page 146* for information on the data merge, import and export functions of the **Subscriber Database**.

The following section explains the advanced features of the **Subscriber Database** dialog when you are inserting a new or editing an existing subscriber.

Subscriber's Advanced Features dialog

Clicking the **[Advanced]** button in the **Edit Subscriber Database** dialog opens the **Edit Subscriber's Advanced Features** dialog window.

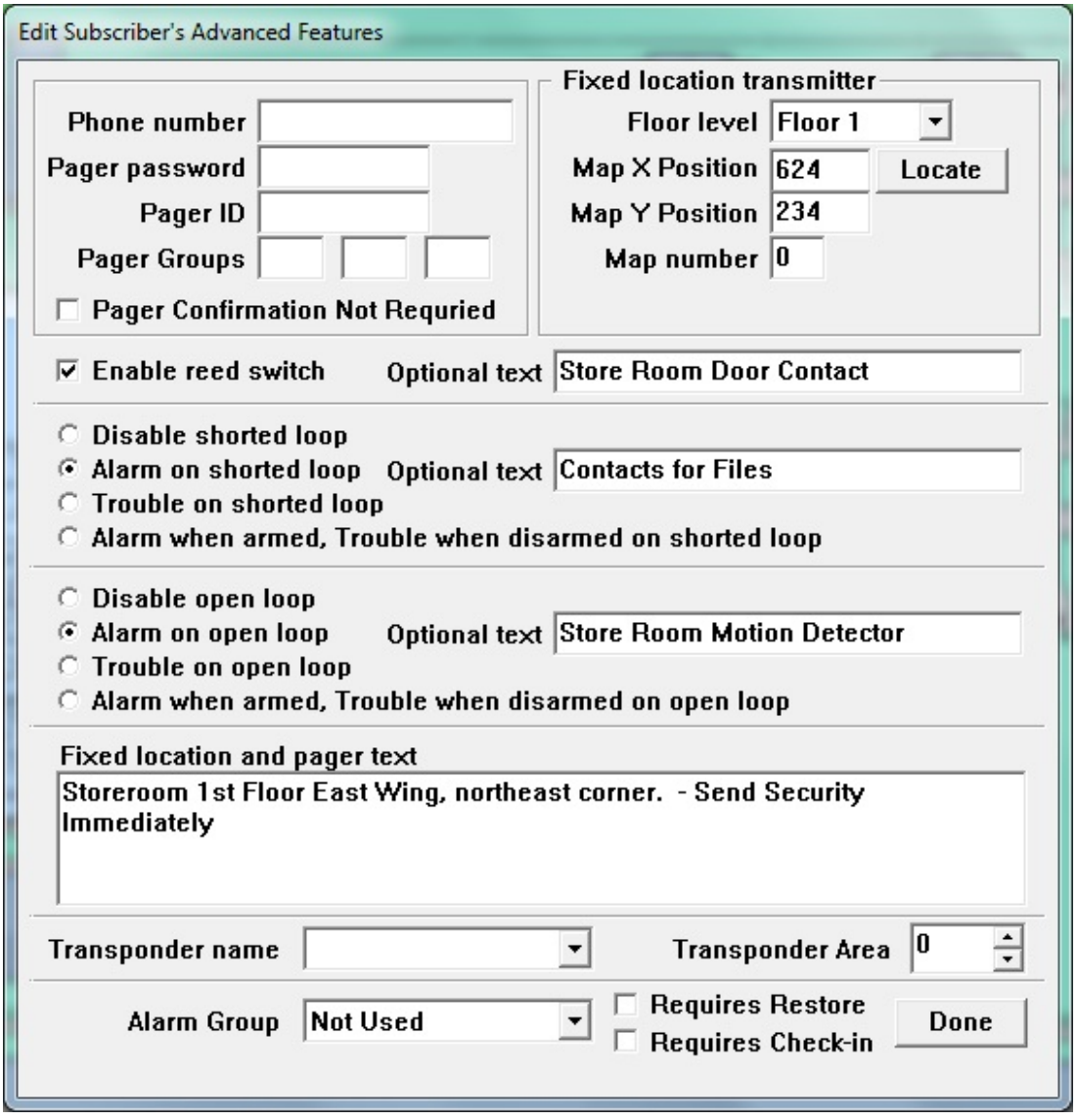


Figure 7.15: Subscriber's Advanced Features Dialog

The **Edit Subscriber's Advanced Features** dialog is used to set up special transmitters that monitor fixed locations, subscriber pager access, parameters for point transmitters, the virtual fence for a wandering alarm, the alarm group for arming of the transmitter and check-in requirements for this transmitter.

Phone number This phone number is dialed to send a pager message to this subscriber. Typically, this is a different phone number than the one that is manually dialed to access this pager. The phone number is assigned by the paging service.

Pager password This is the password to be sent to the paging service when a page is sent to this subscriber. Leave blank if not required (typically the pager password is not required). The pager password is assigned by the paging service.

Pager ID	This is the ID that identifies the pager to receive the pager message (many times this value is the last 7 digits that would be manually dialed to access this pager). The pager ID is assigned by the paging service.
Pager Groups	These are the pager groups that this subscriber is a member of. This subscriber may be a member of up to 3 different pager groups.
Pager Confirmation Not Required	If checked, the confirmation pager message is not sent to this pager if alarm is acknowledged by an acknowledgement transmitter.
Fixed location transmitter	This section is to be used only when this transmitter is mounted in a fixed location (it does not move). When this transmitter transmits and alarm it will always be reported at the programmed location.
Floor level	This is the floor level where this alarm is to be located for a fixed location transmitter.
Map X Position	This is the X coordinate of the map position where this alarm is to be located for a fixed location transmitter.
Map Y Position	This is the Y coordinate of the map position where this alarm is to be located for a fixed location transmitter.
Locate	When clicked, the dialog will disappear and the cursor will change to a cross hair. Moving the cursor to a point on the map and clicking the left mouse button will scroll the map so that point is at the center of the screen. When the map is showing the desired alarm location, move the cross hair to the exact location of the alarm to be reported and click the right mouse button. The dialog will reappear and the selected location will be entered into the X and Y coordinates. If while the cross hair cursor is being displayed, you desire to exit without changing any coordinate values, press the <Esc> key and the transponder edit dialog will reappear.
Map number	Defines which bitmap is to be displayed for the fixed location of this transmitter. The default map is 0, which corresponds to bitmap MAP0.EDB stored in the “Escort” sub-directory. Map 1 would be MAP1.EDB. There can be 100 maps per Security Escort system (0-99).
Enable reed switch	If checked the reed switch input of this transmitter enabled to cause an alarm. Otherwise the reed switch input will be disabled. The alarm group this transmitter is assigned to must be armed, for this input to cause an alarm, which is displayed. If no alarm group is assigned, the transmitter is always armed. For this option to be enabled, the transmitter’s class must be set to “Point type”.
Optional text	This is optional text that will be added to the location text when this input reports an alarm. For this option to be enabled, the transmitter’s class must be set to “Point type”.
Disable on shorted loop	If selected, a shorted loop on this transmitter will not cause an alarm or trouble report to be displayed. For this option to be enabled, the transmitter’s class must be set to “Point type”.

Alarm on shorted loop	If selected and the alarm group, where this transmitter is assigned to, is armed, then a shorted loop on this transmitter will cause an alarm report to be displayed. The alarm group this transmitter is assigned to must be armed, for this input to cause an alarm, which is displayed. If no alarm group is assigned, the transmitter is always armed. For this option to be enabled, the transmitter's class must be set to "Point type".
Trouble on shorted loop	If selected, a shorted loop on this transmitter will cause a trouble report to be displayed. For this option to be enabled, the transmitter's class must be set to "Point type".
Alarm when armed, Trouble when disarmed on shorted loop	If selected and the alarm group, where this transmitter is assigned to, is armed; then a shorted loop on this transmitter will cause an alarm report to be displayed. If selected and the alarm group, where this transmitter is assigned to, is disarmed, then a shorted loop on this transmitter will cause a trouble report to be displayed. If no alarm group is assigned, the transmitter is always armed. For this option to be enabled, the transmitter's class must be set to "Point type".
Disable open loop	If selected, an open loop on this transmitter will not cause an alarm or trouble report to be displayed. For this option to be enabled, the transmitter's class must be set to "Point type".
Alarm on open loop	If selected and the alarm group, where this transmitter is assigned to, is armed, then an open loop on this transmitter will cause an alarm report to be displayed. The alarm group, where this transmitter is assigned to, must be armed for this input to cause an alarm, which is displayed. If no alarm group is assigned, the transmitter is always armed. For this option to be enabled, the transmitter's class must be set to "Point type".
Trouble on open loop	If selected, an open loop on this transmitter will cause a trouble report to be displayed. For this option to be enabled, the transmitter's class must be set to "Point type".
Alarm when armed, Trouble when disarmed on open loop	If selected and the alarm group, where this transmitter is assigned to, is armed; then an open loop on this transmitter will cause an alarm report to be displayed. If selected and the alarm group, where this transmitter is assigned to, is disarmed, then an open loop on this transmitter will cause a trouble report to be displayed. If no alarm group is assigned, the transmitter is always armed. For this option to be enabled, the transmitter's class must be set to "Point type".
Fixed location and pager text	This is the text that will be displayed as the location of the alarm for fixed location transmitters and on pagers reporting this alarm.
Transponder name	Select the transponder with the area that is defined for a wandering (virtual fence) alarm. See **Transponder Area** below for the operation and setup of the wandering alarm (virtual fence alarm).

Transponder Area

Wandering alarm - Create a protected area by placing a virtual monitor “fence” around an area of the main map. These areas are defined in the **Transponder Database**. If this transmitter is constrained to remain within one of these defined areas, first select the defining transponder in **Transponder name** above. Then select the desired area from this drop-down list of the transponder’s area names.
For the wandering alarm to work, the supervision period must also be programmed for this transmitter.
Then specific transmitters are marked in the subscriber database, to be constrained within a specific fenced area defined by this option. If the transmitters leave their defined area, the system will report this as a Wandering alarm and continue to monitor and track the location of the transmitter until the alarm is canceled from the screen in the normal way. However, these tracking updates can only occur every supervision transmission period (not on an accelerated rate like a tracking alarm).
The Security Escort system computes the location of the transmitters when they broadcast automatic supervision transmissions periodically.
Because of the basic location accuracy and the floor-to-floor accuracy of the system, there is a potential for some false alarms. If false alarms are a problem, check the **Filter Virtual Fence** checkbox in the **Security Preferences** dialog. If you do this, two successive location calculations will have to indicate the transmitter has moved outside the protected area before an alarm is generated. The downside of this is a delay in the reporting of a wandering alarm of one extra transmitter supervision period.

Alarm Group

This is the alarm group that controls the arm/disarm status of this transmitter. Select the desired alarm group from the dropdown list of the alarm group names. This alarm group must be armed, for this transmitter to cause an alarm, which is displayed. If no alarm group is assigned, the transmitter is always armed.

Requires Restore

When this checkbox is checked, transmitter will have to be restored.

Requires Check-in When this checkbox is checked, this transmitter will have to be activated once each day during the **Check-in Schedule** time. At the end of the check-in period, if the subscriber fails to check-in, a **Failed to Check-in Report** will be generated and presented to the operator of the software. This report contains all of the people who failed to check-in with their first address line and phone number. All subscribers in the report must be checked on to make sure they are not in need of assistance, as this may be a life-treating situation. A printed report may also be generated.
If the transmitter is not a point type, then the transmitter can generate alarms and therefore a test transmission will be used for the check-in.
If the transmitter is a point type, then any non-trouble transmission will serve as a check-in.
One of the 10 schedules must be selected as the check-in schedule to define the check-in period.

Done Click this button when all changes to this dialog are completed and return the main **Subscriber Database** edit dialog.

7.11 Schedules dialog

This selection informs management of the ten-time of day/day of week schedules and holidays. The top portion of the display shows the ten-time-of-day/day-of-week schedules that Security Escort supports. For each schedule, there is an indication the schedule is currently active or armed (ACT); otherwise, the schedule is disarmed (OFF).

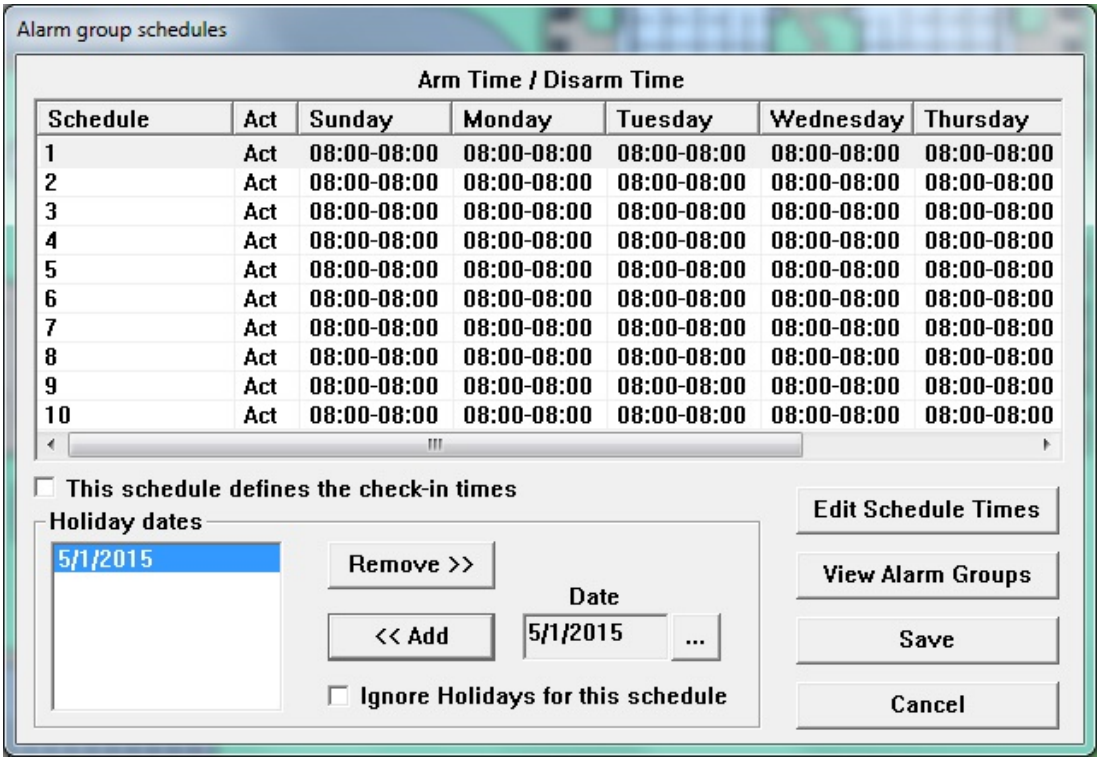


Figure 7.16: Schedule Screen

For each day-of-the-week, the arm time (time the schedule becomes active) and disarm time (time the schedule becomes inactive) are displayed. To edit the arm and disarm times, click the **[Edit Schedule Times]** button. Double clicking the number of the schedule allows you to name the schedules.

This schedule defines the check-in times	One of the ten schedules can be used to define the check-in times for those subscribers that must check-in. Click on the schedule for the check-in schedule, highlighting it. Then check this checkbox, to set the selected schedule as the check-in schedule. Both the arm time and disarm time must be programmed for every day the check-ins must take place. The arm time is the start of the check-in schedule and it must occur before the disarm time that marks the end of the check-in schedule for that day.
[Edit Schedule Times]	Clicking this button displays the **Edit Schedule Times** dialog so the day of week arm and disarm schedule times can be edited.
[View Alarm Groups]	Clicking this button displays the **View Alarm Groups** dialog. This screen shows the alarm groups assigned to the selected schedule and their current arming state.
Ignore Holidays for this Schedule	Each schedule can use the holiday dates as exceptions.

7.11.1 Ignore Holidays for this schedule

Each schedule can use the holiday dates as exceptions. Schedules are activated (armed) following the normal schedules if the holiday dates are configured to be ignored. Otherwise, the schedules are activated the entire day for the holiday dates.

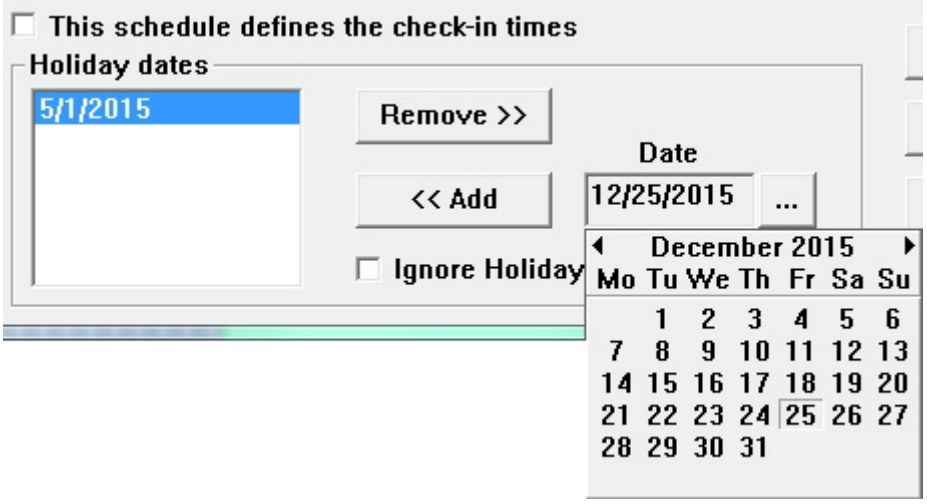


Figure 7.17: Holiday Selection in the Schedule Dialog

Ignore Holidays for this Schedule	If the **Ignore Holidays** checkbox is checked for the indicated holiday dates, the schedules are activated (armed) that entire day. If the **Ignore Holidays** checkbox is not checked, the normal action of the schedules takes place on the holiday dates.
Date [...]	Clicking this button displays a calendar where you can graphically select a date.
[Remove >>]	Clicking this button removes the selected date from the **Holiday dates** list box.
[<< Add]	Clicking this button adds the date shown to the **Holiday dates** list box.

7.11.2 Edit Schedule Times dialog

This dialog allows the arming and disarming times to be programmed for each of the days of the week. All times are expressed in 24-hour time (00:00 to 23:59). Each schedule has one **Arm Time** and one **Disarm Time** for each of the 7 days of the week.
If both the **Arm Time** and **Disarm Time** are programmed to 00:00, the schedule will be active (armed) for the entire day.
If the **Arm Time** is 00:00 and the **Disarm Time** is programmed, the schedule will be active (armed) from midnight to the programmed **Disarm Time**. The schedule will be off (disarmed) from the **Disarm Time** to the end of the day.
If the **Disarm Time** is 00:00 and the **Arm Time** is programmed, the schedule will be off (disarmed) from midnight to the programmed **Arm Time**. The schedule will be active (armed) from the **Arm Time** to the end of the day.

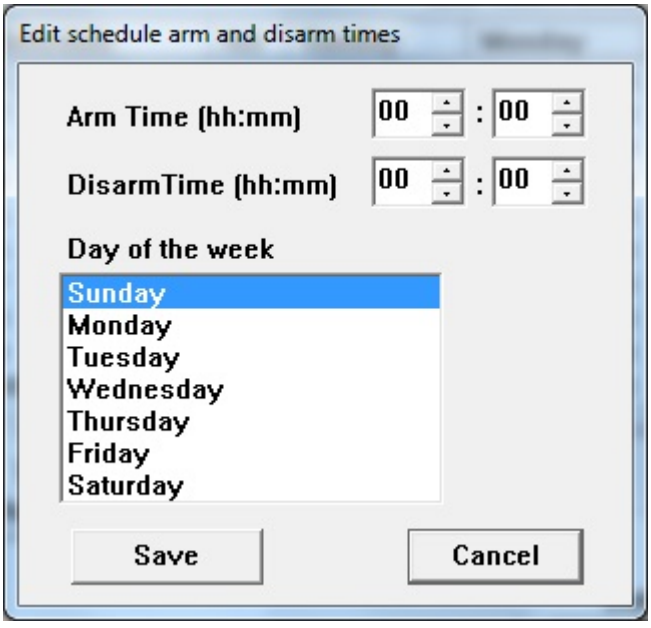


Figure 7.18: Edit Schedule Time dialog

If both the **Disarm Time** and the **Arm Time** are programmed, and the **Disarm Time** occurs before the **Arm Time** (normal 8 to 5 style day), the schedule will be active (armed) from midnight to the programmed **Disarm Time**. The schedule will be off (disarmed) from the **Disarm Time** to the **Arm Time**. The schedule will be active (armed) from the **Arm Time** to the end of the day.
If both the **Disarm Time** and the **Arm Time** are programmed, and the **Arm Time** occurs before the **Disarm Time**, the schedule is off (disarmed) from midnight to the programmed **Arm Time**. The schedule is active (armed) from the **Arm Time** to the **Disarm Time**. The schedule is off (disarmed) from the **Disarm Time** to the end of the day.

Arm Time	This is the time that the schedule becomes active (on or armed) for the selected day of the week. Times are expressed in 24-hour time (00:00 to 23:59).
Disarm Time	This is the time that the schedule goes off (disarmed) for the selected day of the week. Times are expressed in 24-hour time (00:00 to 23:59).
Day of the Week	Select the day you desire to change the time for. The **Arm Time** and **Disarm Time** are programmed separately for each day of the week. You must individually select each day of the week, and set the desired times.

7.11.3 View Alarm Groups dialog

This dialog shows the alarm groups that are assigned to the selected schedule and their current arming state. The “ON” and “OFF” states indicate that the alarm group is under manual control. “AUTO” is under control of the selected schedule. The alarm group will be armed if the schedule is active.

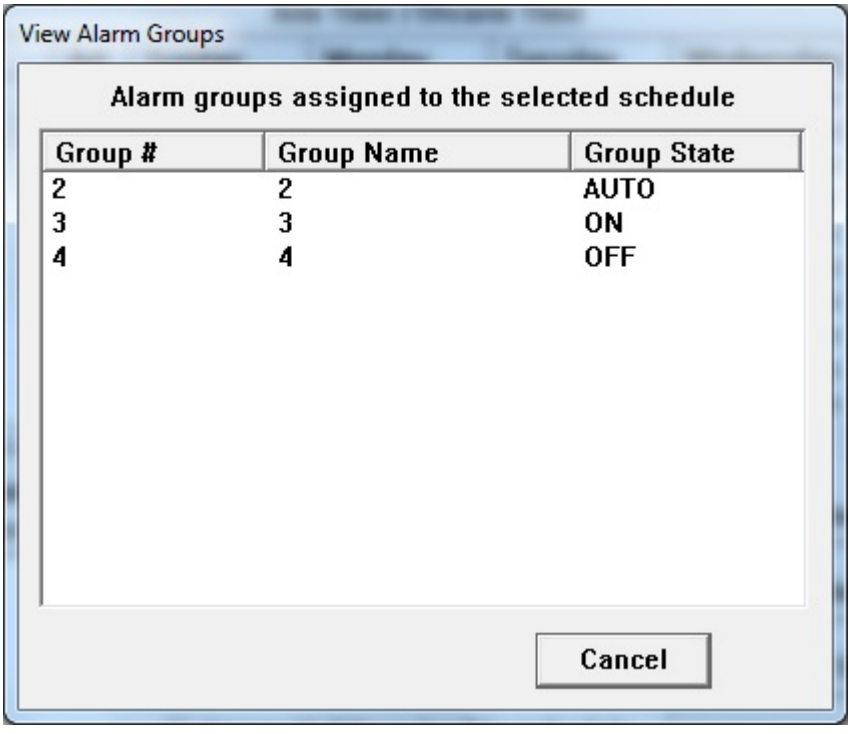


Figure 7.19: View Alarm Groups Dialog

7.11.4 Alarm Groups dialog

This dialog allows setup and arm/disarm control of the 99 alarm groups. Any number of point type transmitters can be assigned to an alarm group in the **Subscriber Database's Advanced** dialog. However, each transmitter can only be assigned to one alarm group.
An alarm group can be manually armed and disarmed, or assigned to a schedule to automatically arm and disarm the alarm group.

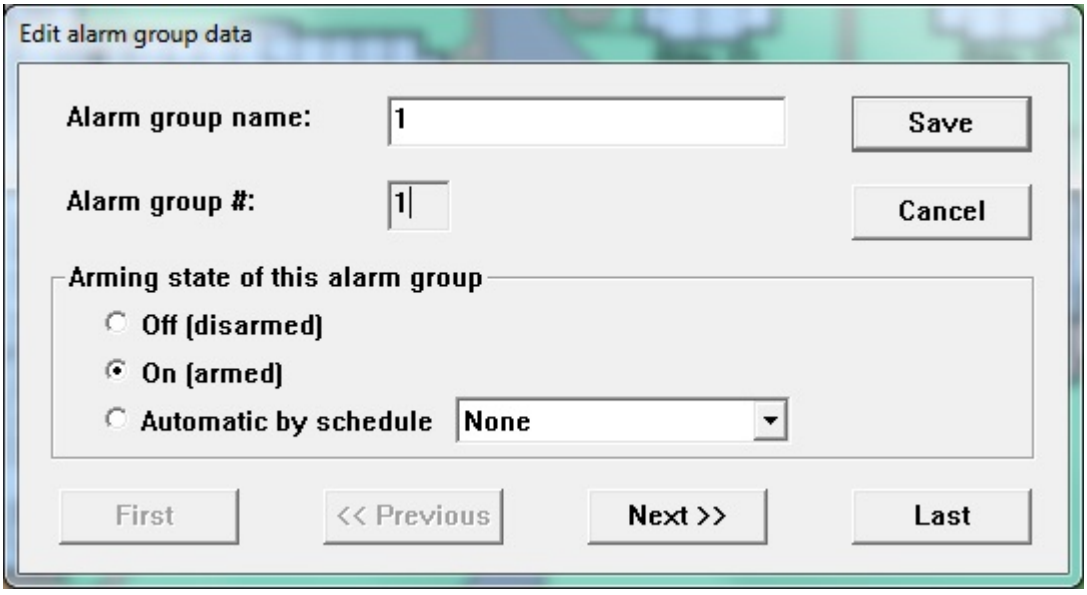


Figure 7.20: Alarm Groups Dialog

Alarm group name	Enter a descriptive name to identify the function of the points in this alarm group.
Alarm group #	This is the number of the alarm group (1-99).
Arming state of this alarm group	The **Off (disarmed)**, **On (armed)** and **Automatic by Schedule** selection control the arming state of this alarm group.
Off (disarmed)	Selecting this option disarms the alarm group. The alarm group will remain off (disarmed) until manually changed in this dialog to **On (armed)** or **Automatic by Schedule**.
On (armed)	Selecting this option arms the alarm group. The alarm group will remain on (armed) until manually changed in this dialog to **Off (disarmed)** or **Automatic by Schedule**.
Automatic by schedule	Selecting this option assigns the alarm group's arming state to be controlled by the indicated schedule. When the schedule is active (on or armed) the alarm group will be armed. When the schedule is off (disarmed) the alarm group will be disarmed. Any number of alarm groups may be assigned to the same schedule.
[First]	Clicking this button takes you to alarm group 1.
[Previous]	Clicking this button takes you to the next lower alarm group from the one currently displayed. It will not wrap around. Therefore, it will be disabled at alarm group 1.

[Next] Clicking this button takes you to the next higher alarm group from the one currently displayed. It will not wrap around. Therefore, it will be disabled at alarm group 99.

[Last] Clicking this button takes you to alarm group 99.

7.11.5 Alarm Group State dialog

This dialog will display a list of the alarm groups that are currently armed, and have one or more transmitters (points) faulted. The points are presented because they were not restored when their automatic schedule armed, or there was an alarm while the alarm group was on.

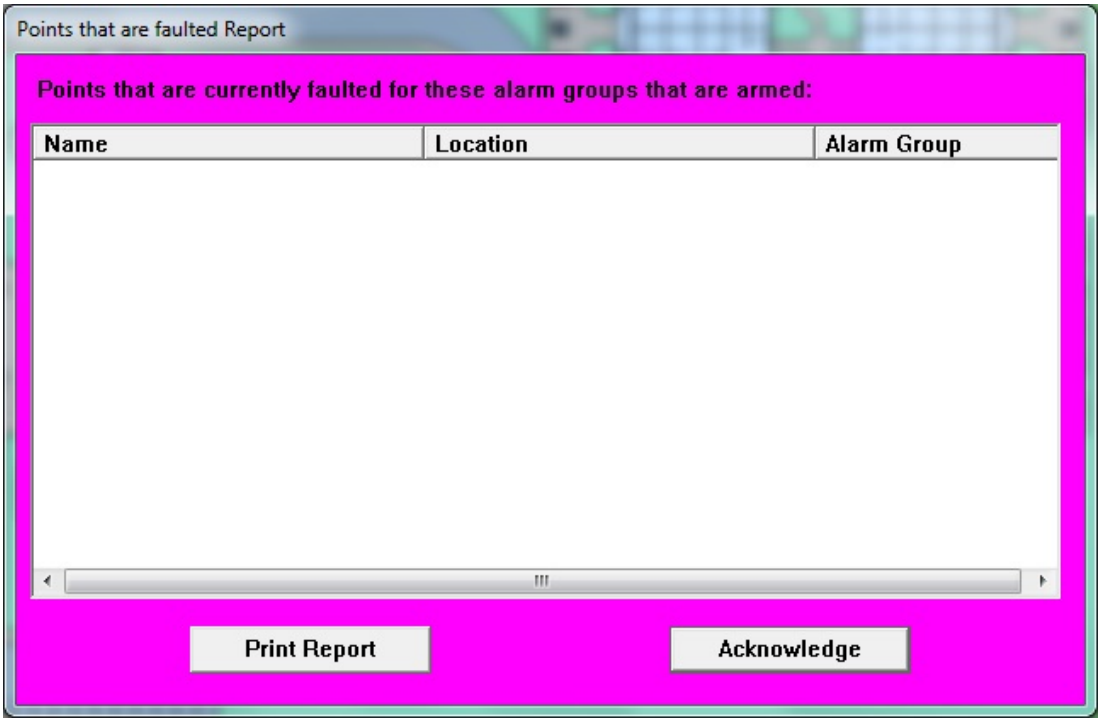


Figure 7.21: Alarm Group State Dialog

[Print Report] Clicking this button prints the displayed data to the report printer.

[Acknowledge] Clicking this button closes the dialog if it was selected from the menu. However, if the dialog was presented automatically at the arm time of an alarm group's automatic schedule because they were not restored, or there was an alarm while the alarm group was on, then you are required to enter your password to acknowledge the dialog, and remove it from this computer's (and all other computer workstations) screens.

7.11.6 Current Check-in Status dialog

This dialog displays a list of subscribers that are required to check-in and failed to do so during the last check-in period. Also shown are their addresses, phone numbers, and the last time they checked-in.

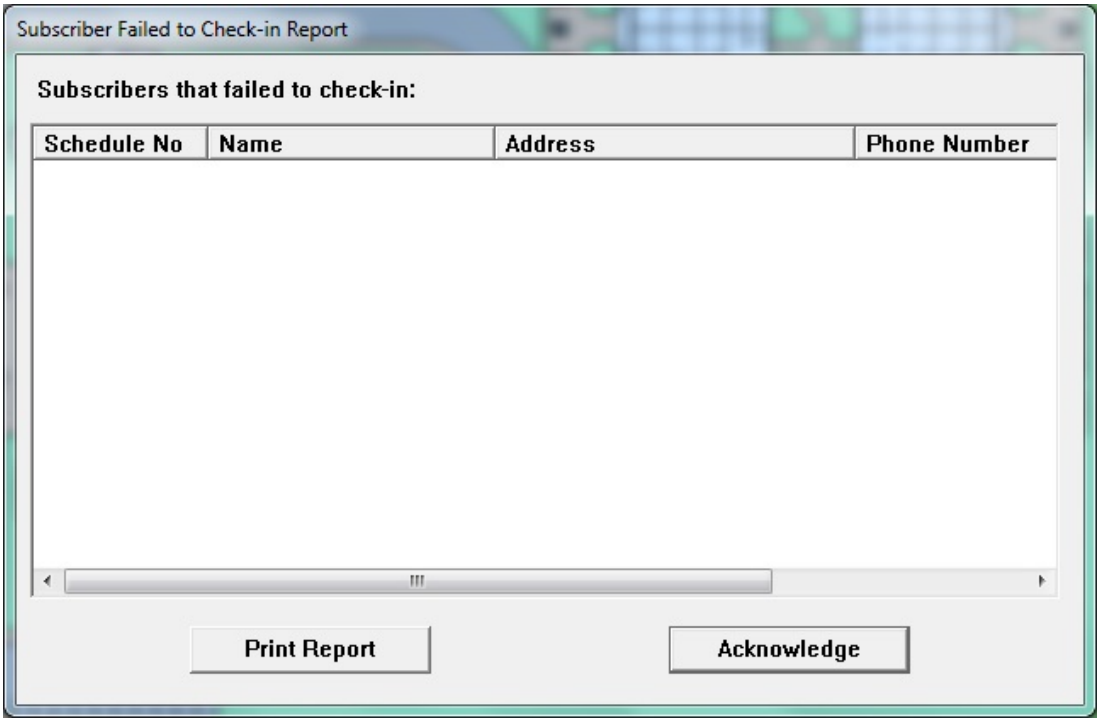


Figure 7.22: Current Check-in Status Dialog

[Print Report] Clicking this button prints the displayed data to the report printer.

[Acknowledge] Clicking this button closes the dialog if it was selected from the menu. However, if the dialog appeared automatically at the end of the check-in period because some subscribers failed to check-in, you must enter your password to acknowledge the dialog and remove it from this computer's (and all other computer workstations) screens.

7.12 Exporting, importing and merging the Subscriber Database

The following sections describe the steps to export, import and merge data from and into the **Subscriber Database**. The file formats for the tasks are included in detail.

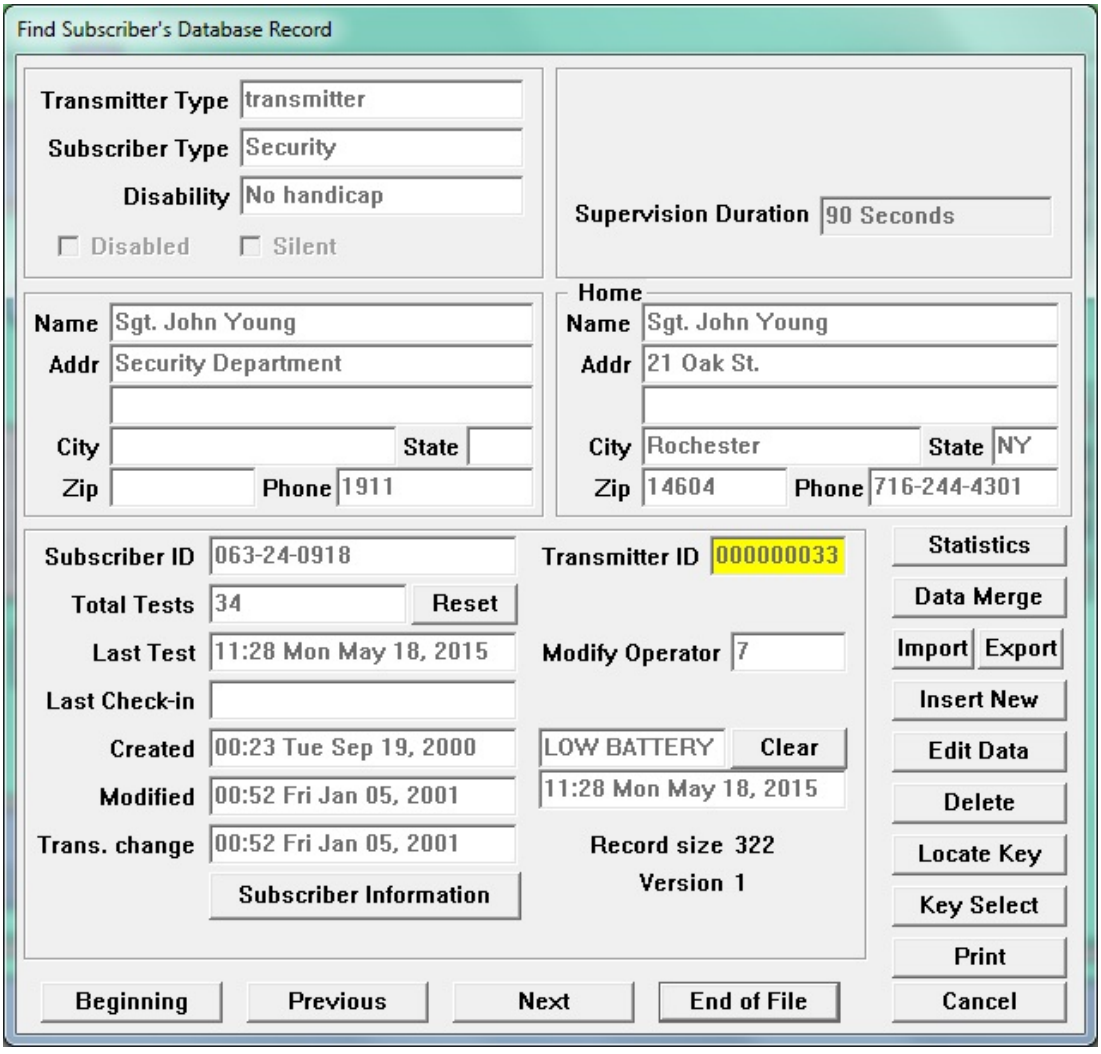


Figure 7.23: Find Subscriber's Database Record Dialog

7.12.1 File format of "TABMERGE.DAT" / "TABMERGE_EXPORT.DAT"

The file of data record entries used for export, import and merge must be in tab delimited text format. For data merge and import, It must be placed in the Security Escort folder (typically “C:\ESCORT”) and named as “TABMERGE.DAT”. For export functionality, the exported file is named as “TABMERGE_EXPORT.DAT”. Both file formats are the same.

The data fields must be in the following order, delimited by the horizontal tab character (decimal 8) and the record must be terminated with a carriage return (decimal 13). If a data field has no data, just store the terminating tab character for that field. The total number of characters in all the fields of a record must be 255 characters or less, including the tab and carriage return characters.

Data fields in required order	Excel Column	Restrictions
Subscriber Name	A	This field may be up to 30 characters. This field may contain any printable ASCII character except the '?'.
Subscriber ID	B	This field may be up to 12 characters. This field may contain only ALPHA, numeric and the dash ASCII characters.
Here Phone Number	C	This field may be up to 16 characters. This field may contain only numeric, '#', '*', '(', ')', comma and the dash ASCII characters.
Here Address 1	D	This field may be up to 30 characters. This field may contain any printable ASCII character except the '?'.
Here Address 2	E	This field may be up to 30 characters. This field may contain any printable ASCII character except the '?'.
Here City	F	This field may be up to 20 characters. This field may contain any printable ASCII character except the '?'.
Here State	G	This field may be up to 3 characters. This field may contain only ALPHA ASCII characters.
Here Zip	H	This field may be up to 10 characters. This field may contain only ALPHA, numeric and the dash ASCII characters.
Away Phone Number	I	This field may be up to 16 characters. This field may contain only numeric, '#', '*', '(', ')', comma and the dash ASCII characters.
Away Address 1	J	This field may be up to 30 characters. This field may contain any printable ASCII character except the '?'.
Away Address 2	K	This field may be up to 30 characters. This field may contain any printable ASCII character except the '?'.
Away City	L	This field may be up to 20 characters. This field may contain any printable ASCII character except the '?'.
Away State	M	This field may be up to 3 characters. This field may contain only ALPHA ASCII characters.
Away Zip	N	This field may be up to 10 characters. This field may contain only ALPHA, numeric and the dash ASCII characters.

Data fields in required order	Excel Column	Restrictions
Supplemental Text Field 1	O	This field may be up to 254 characters. This field may contain any printable ASCII character except the '?'.
Supplemental Text Field 2	P	This field may be up to 254 characters. This field may contain any printable ASCII character except the '?'.
Supplemental Text Field 3	Q	This field may be up to 254 characters. This field may contain any printable ASCII character except the '?'.
Supplemental Text Field 4	R	This field may be up to 254 characters. This field may contain any printable ASCII character except the '?'.
Pager Phone Number	S	This field may be up to 16 characters. This field may contain only numeric, '#', '*', '(', ')', comma and the dash ASCII characters.
Pager Password	T	This field may be up to 6 characters. This field may contain only numeric, and ALPHA ASCII characters.
Pager Pager ID	U	This field may be up to 10 characters. This field may contain only numeric ASCII characters.
Subscriber Type	V	"0 Unclassified", "1 Commuter", "2 Faculty", "3 Resident", "4 Security", "5 Staff", "6 Installer", "7 Out of Service", "8 Watchman", "9 Visitor", "10 Point type", "11 Acknowledgement". This field should contain only numeric ASCII characters.
Handicapped Type	W	"0 No handicap", "1 Blind", "2 Deaf", "3 Handicapped", "4 Wheel chair". This field should contain only numeric ASCII characters.
Transmitter ID	X	This field may be up to 9 characters. This field should contain only numeric ASCII characters.
Away Name	Y	This field may be up to 30 characters. This field may contain any printable ASCII character except the '?'.
Image Filename	Z	This field may be up to 30 characters. This field may contain any printable ASCII character that is valid for a file name.
Height Feet	AA	0-7, This field should contain only numeric ASCII characters.
Height Inches	AB	0-11, This field should contain only numeric ASCII characters.

Data fields in required order	Excel Column	Restrictions
Build Code	AC	"0 Medium", "1 Slim", "2 Large". This field should contain only numeric ASCII characters.
Hair Color	AD	"0 Brown", "1 Auburn", "2 Black", "3 Blond", "4 Brunet", "5 Grey", "6 Red". This field should contain only numeric ASCII characters.
Eye Color	AE	"0 Brown", "1 Blue", "2 Green", "3 Hazel", "4 Grey". This field should contain only numeric ASCII characters.
Pager Group A	AF	0-99, This field should contain only numeric ASCII characters.
Pager Group B	AG	0-99, This field should contain only numeric ASCII characters.
Pager Group C	AH	0-99, This field may contain only numeric ASCII characters.

Data fields in required order	Excel Column	Restrictions
Fixed Floor Level	AI	"0 Basement5", "1 Basement4", "2 Basement3", "3 Basement2", "4 Basement1", "5 Tunnel", "6 Basement ", "7 Ground","8 Outside", "9 Floor 1", "10 Floor 2", "11 Floor 3", "12 Floor 4", "13 Floor 5", "14 Floor 6", "15 Floor 7", "16 Floor 8", "17 Floor 9", "18 Floor 10", "19 Floor 11", "20 Floor 12", "21 Floor 13", "22 Floor 14", "23 Floor 15", "24 Floor 16", "25 Floor 17", "26 Floor 18", "27 Floor 19", "28 Floor 20", "29 Floor 21", "30 Floor 22", "31 Floor 23", "32 Floor 24", "33 Floor 25", "34 Floor 26", "35 Floor 27", "36 Floor 28", "37 Floor 29", "38 Floor 30", "39 Floor 31", "40 Floor 32", "41 Floor 33", "42 Floor 34", "43 Floor 35", "44 Floor 36", "45 Floor 37", "46 Floor 38", "47 Floor 39", “48 Floor 40”, “49 Floor 41”, “50 Floor 42”, “51 Floor 43”, “52 Floor 44”, “53 Floor 45”, “54 Floor 46”, “55 Floor 47”, “56 Floor 48”, “57 Floor 49”, “58 Floor 50”, “59 Floor 51”, “60 Floor 52”, “61 Floor 53”, “62 Floor 54”, “63 Floor 55”, “64 Floor 56”, “65 Floor 57”, “66 Floor 58”, “67 Floor 59”, “68 Floor 60”, “69 Floor 61”, “70 Floor 62”, “71 Floor 63”, “72 Floor 64”, “73 Floor 65”, “74 Floor 66”, “75 Floor 67”, “76 Floor 68”, “77 Floor 69”, “78 Floor 70”, “79 Floor 71”, “80 Floor 72”, “81 Floor 73”, “82 Floor 74”, “83 Floor 75”, “84 Floor 76”, “85 Floor 77”, “86 Floor 78”, “87 Floor 79”, “88 Floor 80”, “89 Floor 81”, “90 Floor 82”, “91 Floor 83”, “92 Floor 84”, “93 Floor 85”, “94 Floor 86”, “95 Floor 87”, “96 Floor 88”, “97 Floor 89”, “98 Floor 90”, “99 Floor 91”, “100 Floor 92”, “101 Floor 93”, “102 Floor 94”, “103 Floor 95”, “104 Floor 96”, “105 Floor 97”, “106 Floor 98”, “107 Floor 99”. This field should contain only numeric ASCII characters.
Fixed Map X Location	AJ	This field may contain only numeric ASCII characters.
Fixed Map Y Location	AK	This field may contain only numeric ASCII characters.
Fixed Bitmap Number	AL	0-99 This field may contain only numeric ASCII characters.

Data fields in required order	Excel Column	Restrictions
Supervision Interval	AM	“0 None”, “1 is 90 Second Supervision”, “2 is 30 Second Supervision”, “3 is 1 Hour Supervision. This field may contain only numeric ASCII characters.
Alarm Group	AN	0-99, This field may contain only numeric ASCII characters.
Shorted Loop	AO	This field may contain only numeric ASCII characters.
Open Loop	AP	This field may contain only numeric ASCII characters.
Status	AQ	Encoded value. Do not change.
Enable Magnetic Reed	AR	This field may contain only numeric ASCII characters.
Fixed Location Text	AS	This field may be up to 254 characters. This field may contain any printable ASCII character except the ‘?’
Magnetic Reed Text	AT	This field may be up to 30 characters. This field may contain any printable ASCII character except the ‘?’
Shorted Loop Text	AU	This field may be up to 30 characters. This field may contain any printable ASCII character except the ‘?’
Open Loop Text	AV	This field may be up to 30 characters. This field may contain any printable ASCII character except the ‘?’
Status Flags	AW	Encoded value. Do not change.
Modify Op	AX	0-30000, This field may contain only numeric ASCII characters.
Test Time	AY	Encoded 32-bit time value. Do not change.
Last Transmitter Change	AZ	Encoded 32-bit time value. Do not change.
Spare Date	BA	Encoded 32-bit time value. Do not change.
Last Fail To Test Letter	BB	Encoded 32-bit time value. Do not change.
Created	BC	Encoded 32-bit time value. Do not change.
Modified	BD	Encoded 32-bit time value. Do not change.
Low Battery	BE	Encoded 32-bit time value. Do not change.
Spare2	BF	This field should be blank.
Spare3	BG	This field should be blank.

7.12.2 Exporting the Subscriber Database

This section describes the information required to export data from the **Subscriber Database**.

Notice!
There is no way to undo the operations. Therefore, it is recommended to **perform a database backup** prior to starting the task. Upon completion of the task, verify the updated data before the new database is placed in service. If there are problems, restore the **Subscriber Database** from the backup.

To import or merge data from the import/merge file, you will need to format the data and columns according to a specific format. To simplify the preparation, it is recommended that you perform the export function first, so that you can use the exported file as your template for your data import/merge. You will need to rename the file from “TABMERGE_EXPORT.DAT” to “TABMERGE.DAT” accordingly.
Only users or operators who are assigned the minimum security level of “View Subscribers” are able to view the **Subscriber Database**. Go to menu **File >Subscriber Database** dialog, and click the **[Export]** button.

Notice!
Important! The export operation does not change the existing records in **Subscriber Database**. However, be mindful that every time you perform the export function (clicking the **[Export]** button), the operation will overwrite the “TABMERGE_EXPORT.DAT” file.

Be patient, as it may take a while, and watch for the disk activity to stop. If the export is successful, a confirmation dialog appears. You will find the “TABMERGE_EXPORT.DAT” file in the Security Escort folder (typically “C:\ESCORT”).

7.12.3 Importing the Subscriber Database

This section describes the information required to import data into the **Subscriber Database**.

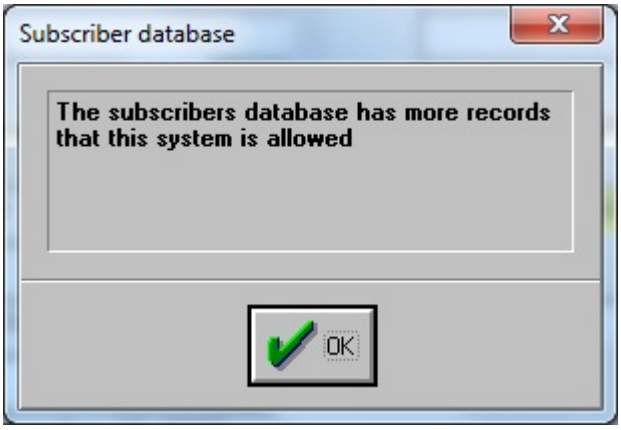
Notice!
There is no way to undo the operations. Therefore, it is recommended to **perform a database backup** prior to starting the task. Upon completion of the task, verify the updated data before the new database is placed in service. If there are problems, restore the **Subscriber Database** from the backup.

Notice!

Important!

Proceeding with the import operation will delete all existing records in **Subscriber Database**. The record entries in “TABMERGE.DAT” are then imported to the **Subscriber Database,** validated and sorted by the **Subscriber ID**.

The number of record entries that is imported is subject to the number of subscribers allowed for the purchased license. You can find this limit in the menu **About > About...** If this limit is reached during the import, a pop-up message appears to inform the user.



The **[Import]** button is only visible to users or operators who are assigned the minimum security level of “Install”, and if the file to import is named accordingly in the correct folder. The file of data record entries must be placed in the Security Escort folder (typically “C:\ESCORT”) and named as “TABMERGE.DAT”.

After preparing the “TABMERGE.DAT” file in the Security Escort folder, start the Security Escort software. Go to menu **File > Subscriber Database** dialog, and click the **[Import]** button. A popup dialog appears asking for confirmation to proceed with the import or to abort the operation.

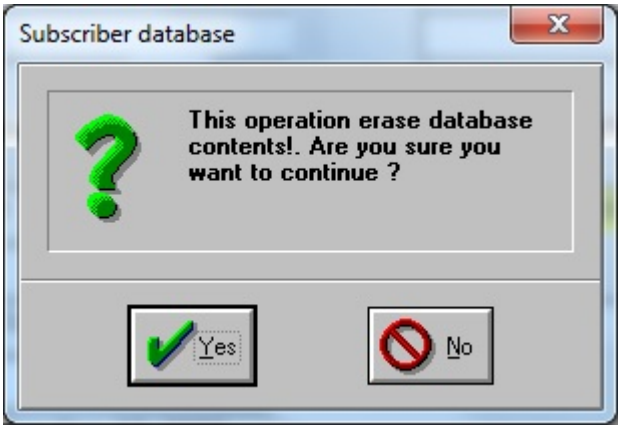


Figure 7.24: Subscriber Database Import Confirmation Dialog

Click the **[Yes]** button to continue. Otherwise, click the **[No]** button to abort. Be patient, as it may take a while, and watch for the disk activity to stop. If the data is imported successfully, a pop-up confirmation message appears. It is a good idea to remove the “TABMERGE.DAT” file, to disable the import feature (the **[Import]** button becomes invisible). If the data is not imported successful, a pop-up error message appears. The error message will indicate the likely issue causing the import to fail.

7.12.4 Merging the Subscriber Database

This section describes the information required to merge data into the **Subscriber Database**.

Notice!

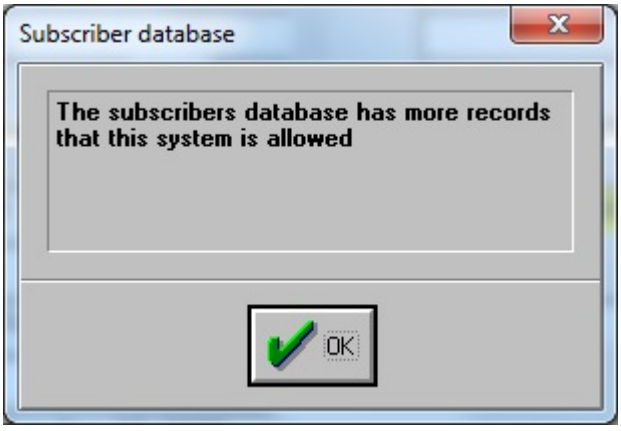
There is no way to undo the operations. Therefore, it is recommended to **perform a database backup** prior to starting the task. Upon completion of the task, verify the updated data before the new database is placed in service. If there are problems, restore the **Subscriber Database** from the backup.

Notice!

Important!

The record entries in the “TABMERGE.DAT” are merged with existing records in the **Subscriber Database**. If the **Subscriber ID** field in the file matches a record in the **Subscriber Database**, the existing record will be merged with the corresponding record entry in the file. Unmatched records will be inserted into the **Subscriber Database** as new records.

The total number of records is subject to the number of subscribers allowed for the purchased license. You can find this limit in the menu **About > About...** If this limit is reached during the merge, a pop-up message appears to inform the user.



The **[Data Merge]** button is only visible to users or operators who are assigned the minimum security level of “Install”, and if the file to import is named accordingly in the correct folder. The file of data record entries must be placed in the Security Escort folder (typically “C:\ESCORT”) and named as “TABMERGE.DAT”.

After preparing the “TABMERGE.DAT” file in the Security Escort folder, start the Security Escort software. Go to menu **File > Subscriber Database** dialog, and click the **[Data Merge]** button.

Be patient, as it may take a while, and watch for the disk activity to stop. If the data is merged successfully, a pop-up confirmation message appears. It is a good idea to remove the “TABMERGE.DAT” file, to disable the merge feature (the **[Data Merge]** button becomes invisible).

7.13 Exporting and importing the Transponder Database

The following sections describe the steps to export and import data from and into the **Transponder Database**. The file formats for the tasks are included in detail.

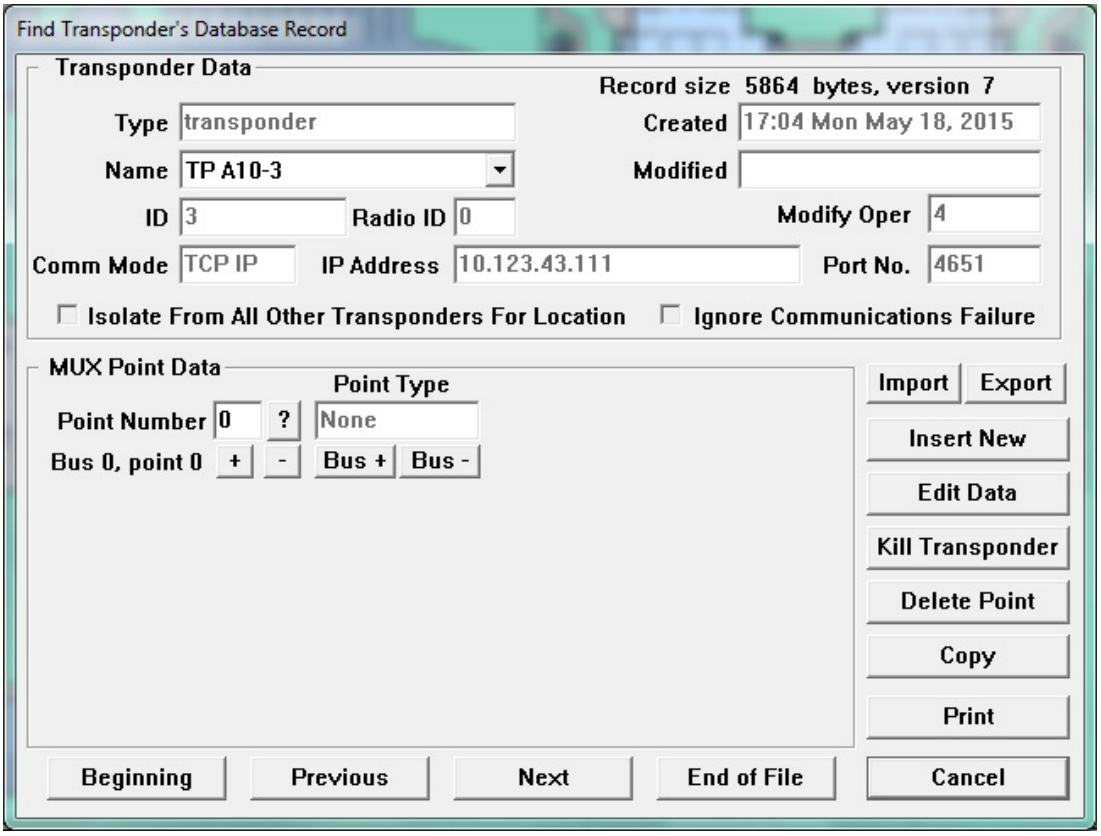


Figure 7.25: Find Transponder's Database Record Dialog

7.13.1 File format of "TRANSMERGE.DAT" / "TRANSMERGE_EXPORT.DAT"

The file of data record entries must be in tab delimited text format. For import functionality, It must be placed in the Security Escort folder (typically “C:\ESCORT”) and named as “TRANSMERGE.DAT”. For export functionality, the exported file is named as “TRANSMERGE_EXPORT.DAT”. Both file formats are the same.
The data fields must be in the following order, delimited by the horizontal tab character (decimal 8) and the record must be terminated with a carriage return (decimal 13). If a data field has no data, just store the terminating tab character for that field. The total number of characters in all the fields of a record must be 255 characters or less, including the tab and carriage return characters.

Notice!
Area data of the transponders is not supported. Only point data of the transponders is used for the export and import functionalities.

Data fields in required order	Excel Column	Restrictions
Transponder ID	A	1-255. This field should contain only numeric ASCII characters.
Coordinator ID	B	Reserved for future use, this field should contain only the numeric 0.

Data fields in required order	Excel Column	Restrictions
Transponder Name	C	This field may be up to 24 characters. This field may contain any printable ASCII character except the '?'
IP Connected	D	"0 RS232", "1 TCP IP". This field should contain only numeric ASCII characters.
Coordinator	E	0. Reserved for future use, this field should contain only the numeric "0".
IP Address	F	This field is blank if **IP Connected** is 0 (RS232). This field should contain a valid IP address if **IP Connected** is 1 (TCP .IP).
Port Number	G	This field is blank if **IP Connected** is 0 (RS232). This field should contain only numeric ASCII characters, 1-65535.
Comm Port Index	H	This field used only if **IP Connected** is 0 (TCP IP). "0 A", "1 B", "2 C", "3 D", "4 E", "5 F", "6 G", "7 H", "8 I", "9 J", "10 K", "11 L"
Ignore Communications Failure	I	This field is 0 if this is not selected. This field is 1 if this is selected. This field should contain only numeric ASCII characters.
Isolate For Location	J	This field is 0 if this is not selected. This field is 1 if this is selected. This field should contain only numeric ASCII characters.
Trouble Text	K	This field may be up to 40 characters. This field may contain any printable ASCII character except the '?'.
Tamper Text	L	This field may be up to 40 characters. This field may contain any printable ASCII character except the '?'.
Trouble Response	M	This field may be up to 135 characters. This field may contain any printable ASCII character except the '?'
Point Number 0	N	This field must be 0 (the point number). This field should contain only numeric ASCII characters.
Point Type	O	"0 receiver", "1 Alert unit", "2 Virtual", "7 None". This field should contain only numeric ASCII characters.
Algorithm Number	P	"0 Default", "1 Classic". "2 Linear", "3 Low", "4 Medium", "5 Strong". This field should contain only numeric ASCII characters.

Data fields in required order	Excel Column	Restrictions
Floor	Q	"0 Basement5", "1 Basement4", "2 Basement3", "3 Basement2", "4 Basement1", "5 Tunnel", "6 Basement ", "7 Ground","8 Outside", "9 Floor 1", "10 Floor 2", "11 Floor 3", "12 Floor 4", "13 Floor 5", "14 Floor 6", "15 Floor 7", "16 Floor 8", "17 Floor 9", "18 Floor 10", "19 Floor 11", "20 Floor 12", "21 Floor 13", "22 Floor 14", "23 Floor 15", "24 Floor 16", "25 Floor 17", "26 Floor 18", "27 Floor 19", "28 Floor 20", "29 Floor 21", "30 Floor 22", "31 Floor 23", "32 Floor 24", "33 Floor 25", "34 Floor 26", "35 Floor 27", "36 Floor 28", "37 Floor 29", "38 Floor 30", "39 Floor 31", "40 Floor 32", "41 Floor 33", "42 Floor 34", "43 Floor 35", "44 Floor 36", "45 Floor 37", "46 Floor 38", "47 Floor 39", “48 Floor 40”, “49 Floor 41”, “50 Floor 42”, “51 Floor 43”, “52 Floor 44”, “53 Floor 45”, “54 Floor 46”, “55 Floor 47”, “56 Floor 48”, “57 Floor 49”, “58 Floor 50”, “59 Floor 51”, “60 Floor 52”, “61 Floor 53”, “62 Floor 54”, “63 Floor 55”, “64 Floor 56”, “65 Floor 57”, “66 Floor 58”, “67 Floor 59”, “68 Floor 60”, “69 Floor 61”, “70 Floor 62”, “71 Floor 63”, “72 Floor 64”, “73 Floor 65”, “74 Floor 66”, “75 Floor 67”, “76 Floor 68”, “77 Floor 69”, “78 Floor 70”, “79 Floor 71”, “80 Floor 72”, “81 Floor 73”, “82 Floor 74”, “83 Floor 75”, “84 Floor 76”, “85 Floor 77”, “86 Floor 78”, “87 Floor 79”, “88 Floor 80”, “89 Floor 81”, “90 Floor 82”, “91 Floor 83”, “92 Floor 84”, “93 Floor 85”, “94 Floor 86”, “95 Floor 87”, “96 Floor 88”, “97 Floor 89”, “98 Floor 90”, “99 Floor 91”, “100 Floor 92”, “101 Floor 93”, “102 Floor 94”, “103 Floor 95”, “104 Floor 96”, “105 Floor 97”, “106 Floor 98”, “107 Floor 99”. This field should contain only numeric ASCII characters.
Alert Unit 1	R	This field contains the Transponder ID of the alert unit. If this is not configured, this field is 0. This field should contain only numeric ASCII characters.
Alert Unit 1 Point	S	This field contains the alert unit point number. If this is not configured, this field is -1. This field should contain only numeric ASCII characters.

Data fields in required order	Excel Column	Restrictions
Alert Unit 2	T	This field contains the Transponder ID of the alert unit. If this is not configured, this field is 0. This field should contain only numeric ASCII characters.
Alert Unit 2 Point	U	This field contains the alert unit point number. If this is not configured, this field is -1. This field should contain only numeric ASCII characters.
Alert Unit 3	V	This field contains the Transponder ID of the alert unit. If this is not configured, this field is 0. This field should contain only numeric ASCII characters.
Alert Unit 3 Point	W	This field contains the alert unit point number. If this is not configured, this field is -1. This field should contain only numeric ASCII characters.
Alert Unit Test	X	This field contains the Transponder ID of the alert unit. If this is not configured, this field is 0. This field should contain only numeric ASCII characters.
Alert Unit Test Point	Y	This field contains the alert unit point number. If this is not configured, this field is -1. This field should contain only numeric ASCII characters.
Point Location Text	Z	This field may be up to 100 characters. This field may contain any printable ASCII character except the '?'.
Map X Position	AA	X position of the point on the map. Default is 0. This field should contain only numeric ASCII characters.
Map Y Position	AB	Y position of the point on the map. Default is 0. This field should contain only numeric ASCII characters.
Sensitivity Adjust	AC	0-99. This field should contain only numeric ASCII characters.
Bitmap Number	AD	0-99. This field should contain only numeric ASCII characters.
Point Number 1	AE	This field must be 1 (the point number). This field should contain only numeric ASCII characters.
Point Type	AF	"0 receiver", "1 Alert unit", "2 Virtual", "7 None". This field should contain only numeric ASCII characters.

Data fields in required order	Excel Column	Restrictions
Algorithm Number	AG	“0 Default”, “1 Classic”. “2 Linear”, “3 Low”, “4 Medium”, “5 Strong”. This field should contain only numeric ASCII characters.
Floor	AH	"0 Basement5", "1 Basement4", "2 Basement3", "3 Basement2", "4 Basement1", "5 Tunnel", "6 Basement ", "7 Ground","8 Outside", "9 Floor 1", "10 Floor 2", "11 Floor 3", "12 Floor 4", "13 Floor 5", "14 Floor 6", "15 Floor 7", "16 Floor 8", "17 Floor 9", "18 Floor 10", "19 Floor 11", "20 Floor 12", "21 Floor 13", "22 Floor 14", "23 Floor 15", "24 Floor 16", "25 Floor 17", "26 Floor 18", "27 Floor 19", "28 Floor 20", "29 Floor 21", "30 Floor 22", "31 Floor 23", "32 Floor 24", "33 Floor 25", "34 Floor 26", "35 Floor 27", "36 Floor 28", "37 Floor 29", "38 Floor 30", "39 Floor 31", "40 Floor 32", "41 Floor 33", "42 Floor 34", "43 Floor 35", "44 Floor 36", "45 Floor 37", "46 Floor 38", "47 Floor 39", “48 Floor 40”, “49 Floor 41”, “50 Floor 42”, “51 Floor 43”, “52 Floor 44”, “53 Floor 45”, “54 Floor 46”, “55 Floor 47”, “56 Floor 48”, “57 Floor 49”, “58 Floor 50”, “59 Floor 51”, “60 Floor 52”, “61 Floor 53”, “62 Floor 54”, “63 Floor 55”, “64 Floor 56”, “65 Floor 57”, “66 Floor 58”, “67 Floor 59”, “68 Floor 60”, “69 Floor 61”, “70 Floor 62”, “71 Floor 63”, “72 Floor 64”, “73 Floor 65”, “74 Floor 66”, “75 Floor 67”, “76 Floor 68”, “77 Floor 69”, “78 Floor 70”, “79 Floor 71”, “80 Floor 72”, “81 Floor 73”, “82 Floor 74”, “83 Floor 75”, “84 Floor 76”, “85 Floor 77”, “86 Floor 78”, “87 Floor 79”, “88 Floor 80”, “89 Floor 81”, “90 Floor 82”, “91 Floor 83”, “92 Floor 84”, “93 Floor 85”, “94 Floor 86”, “95 Floor 87”, “96 Floor 88”, “97 Floor 89”, “98 Floor 90”, “99 Floor 91”, “100 Floor 92”, “101 Floor 93”, “102 Floor 94”, “103 Floor 95”, “104 Floor 96”, “105 Floor 97”, “106 Floor 98”, “107 Floor 99”. This field should contain only numeric ASCII characters.
Alert Unit 1	AI	This field contains the Transponder ID of the alert unit. If this is not configured, this field is 0. This field should contain only numeric ASCII characters.

Data fields in required order	Excel Column	Restrictions
Alert Unit 1 Point	AJ	This field contains the alert unit point number. If this is not configured, this field is -1. This field should contain only numeric ASCII characters.
Alert Unit 2	AK	This field contains the Transponder ID of the alert unit. If this is not configured, this field is 0. This field should contain only numeric ASCII characters.
Alert Unit 2 Point	AL	This field contains the alert unit point number. If this is not configured, this field is -1. This field should contain only numeric ASCII characters.
Alert Unit 3	AM	This field contains the Transponder ID of the alert unit. If this is not configured, this field is 0. This field should contain only numeric ASCII characters.
Alert Unit 3 Point	AN	This field contains the alert unit point number. If this is not configured, this field is -1. This field should contain only numeric ASCII characters.
Alert Unit Test	AO	This field contains the Transponder ID of the alert unit. If this is not configured, this field is 0. This field should contain only numeric ASCII characters.
Alert Unit Test Point	AP	This field contains the alert unit point number. If this is not configured, this field is -1. This field should contain only numeric ASCII characters.
Point Location Text	AQ	This field may be up to 100 characters. This field may contain any printable ASCII character except the '?'.
Map X Position	AR	X position of the point on the map. Default is 0. This field should contain only numeric ASCII characters.
Map Y Position	AS	Y position of the point on the map. Default is 0. This field should contain only numeric ASCII characters.
Sensitivity Adjust	AT	0-99. This field should contain only numeric ASCII characters.
Bitmap Number	AU	0-99. This field should contain only numeric ASCII characters.
. . .		

Data fields in required order	Excel Column	Restrictions
Point Number 63	AOS	This field must be 63 (the point number). This field should contain only numeric ASCII characters.
Point Type	AOT	“0 receiver”, “1 Alert unit”, “2 Virtual”, “7 None”. This field should contain only numeric ASCII characters.
Algorithm Number	AOU	“0 Default”, “1 Classic”. “2 Linear”, “3 Low”, “4 Medium”, “5 Strong”. This field should contain only numeric ASCII characters.
Floor	AOV	"0 Basement5", "1 Basement4", "2 Basement3", "3 Basement2", "4 Basement1", "5 Tunnel", "6 Basement ", "7 Ground","8 Outside", "9 Floor 1", "10 Floor 2", "11 Floor 3", "12 Floor 4", "13 Floor 5", "14 Floor 6", "15 Floor 7", "16 Floor 8", "17 Floor 9", "18 Floor 10", "19 Floor 11", "20 Floor 12", "21 Floor 13", "22 Floor 14", "23 Floor 15", "24 Floor 16", "25 Floor 17", "26 Floor 18", "27 Floor 19", "28 Floor 20", "29 Floor 21", "30 Floor 22", "31 Floor 23", "32 Floor 24", "33 Floor 25", "34 Floor 26", "35 Floor 27", "36 Floor 28", "37 Floor 29", "38 Floor 30", "39 Floor 31", "40 Floor 32", "41 Floor 33", "42 Floor 34", "43 Floor 35", "44 Floor 36", "45 Floor 37", "46 Floor 38", "47 Floor 39", “48 Floor 40”, “49 Floor 41”, “50 Floor 42”, “51 Floor 43”, “52 Floor 44”, “53 Floor 45”, “54 Floor 46”, “55 Floor 47”, “56 Floor 48”, “57 Floor 49”, “58 Floor 50”, “59 Floor 51”, “60 Floor 52”, “61 Floor 53”, “62 Floor 54”, “63 Floor 55”, “64 Floor 56”, “65 Floor 57”, “66 Floor 58”, “67 Floor 59”, “68 Floor 60”, “69 Floor 61”, “70 Floor 62”, “71 Floor 63”, “72 Floor 64”, “73 Floor 65”, “74 Floor 66”, “75 Floor 67”, “76 Floor 68”, “77 Floor 69”, “78 Floor 70”, “79 Floor 71”, “80 Floor 72”, “81 Floor 73”, “82 Floor 74”, “83 Floor 75”, “84 Floor 76”, “85 Floor 77”, “86 Floor 78”, “87 Floor 79”, “88 Floor 80”, “89 Floor 81”, “90 Floor 82”, “91 Floor 83”, “92 Floor 84”, “93 Floor 85”, “94 Floor 86”, “95 Floor 87”, “96 Floor 88”, “97 Floor 89”, “98 Floor 90”, “99 Floor 91”, “100 Floor 92”, “101 Floor 93”, “102 Floor 94”, “103 Floor 95”, “104 Floor 96”, “105 Floor 97”, “106 Floor 98”, “107 Floor 99”. This field should contain only numeric ASCII characters.

Data fields in required order	Excel Column	Restrictions
Alert Unit 1	AOW	This field contains the Transponder ID of the alert unit. If this is not configured, this field is 0. This field should contain only numeric ASCII characters.
Alert Unit 1 Point	AOX	This field contains the alert unit point number. If this is not configured, this field is -1. This field should contain only numeric ASCII characters.
Alert Unit 2	AOY	This field contains the Transponder ID of the alert unit. If this is not configured, this field is 0. This field should contain only numeric ASCII characters.
Alert Unit 2 Point	AOZ	This field contains the alert unit point number. If this is not configured, this field is -1. This field should contain only numeric ASCII characters.
Alert Unit 3	APA	This field contains the Transponder ID of the alert unit. If this is not configured, this field is 0. This field should contain only numeric ASCII characters.
Alert Unit 3 Point	APB	This field contains the alert unit point number. If this is not configured, this field is -1. This field should contain only numeric ASCII characters.
Alert Unit Test	APC	This field contains the Transponder ID of the alert unit. If this is not configured, this field is 0. This field should contain only numeric ASCII characters.
Alert Unit Test Point	APD	This field contains the alert unit point number. If this is not configured, this field is -1. This field should contain only numeric ASCII characters.
Point Location Text	APE	This field may be up to 100 characters. This field may contain any printable ASCII character except the '?'.
Map X Position	APF	X position of the point on the map. Default is 0. This field should contain only numeric ASCII characters.
Map Y Position	APG	Y position of the point on the map. Default is 0. This field should contain only numeric ASCII characters.
Sensitivity Adjust	APH	0-99. This field should contain only numeric ASCII characters.
Bitmap Number	API	0-99. This field should contain only numeric ASCII characters.

7.13.2 Exporting the Transponder Database

This section describes the information required to export data from the **Transponder Database**.

Notice!
There is no way to undo the operations. Therefore, it is recommended to **perform a database backup** prior to starting the task. Upon completion of the task, verify the updated data before the new database is placed in service. If there are problems, restore the **Transponder Database** from the backup.

To import data from the import file, you will need to format the data and columns according to a specific format. To simplify the preparation, it is recommended that you perform the export function first, so that you can use the exported file as your template for your data import. You will need to rename the file from “TRANSMERGE_EXPORT.DAT” to “TRANSMERGE.DAT” accordingly.
Only users or operators who are assigned the minimum security level of “Install” is able to view the **Transponder Database**. Go to menu **File > Transponder Database** dialog, and click the **[Export]** button.

Notice!
Important! The export operation does not change the existing records in **Transponder Database**. However, be mindful that every time you perform the export function (clicking the **[Export]** button), the operation will overwrite the “TRANSMERGE_EXPORT.DAT” file.

Be patient, as it may take a while, and watch for the disk activity to stop. If the export is successful, a confirmation dialog appears. You will find the “TRANSMERGE_EXPORT.DAT” file in the Security Escort folder (typically “C:\ESCORT”).

7.13.3 Importing the Transponder Database

This section describes the information required to import data into the **Transponder Database**.

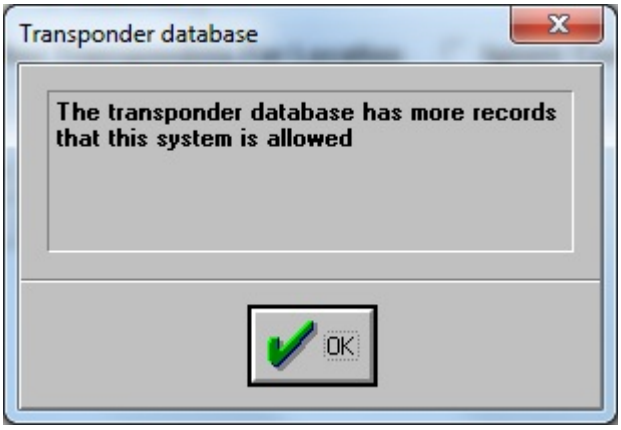
Notice!
There is no way to undo the operations. Therefore, it is recommended to **perform a database backup** prior to starting the task. Upon completion of the task, verify the updated data before the new database is placed in service. If there are problems, restore the **Transponder Database** from the backup.

Notice!

Important!

Proceeding with the import operation will delete all existing records in **Transponder Database**. The record entries in “TRANSMERGE.DAT” are then imported to the **Transponder Database,** validated by the **Transponder ID**.

The number of record entries that is imported is subject to the number of transponders allowed for the purchased license. You can find this limit in the menu **About > About...** If this limit is reached during the import, a pop-up message appears to inform the user.



Only users or operators who are assigned the minimum security level of “Install” is able to view the **Transponder Database**. The file of data record entries must be placed in the Security Escort folder (typically “C:\ESCORT”) and named as “TRANSMERGE.DAT”.

After preparing the “TRANSMERGE.DAT” file in the Security Escort folder, start the Security Escort software. Go to menu **File > Transponder Database** dialog, and click the **[Import]** button. A popup dialog appears asking for confirmation to proceed with the import or to abort the operation.

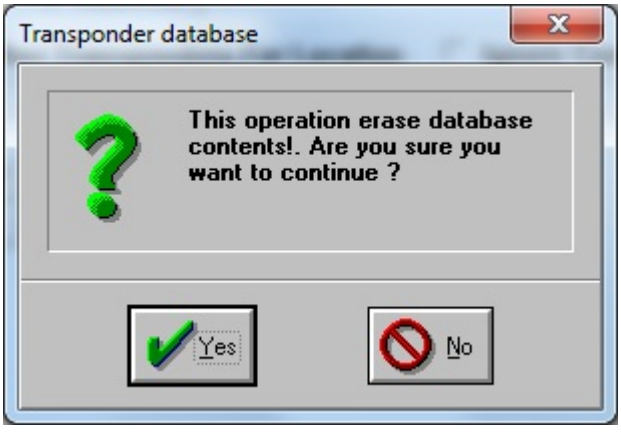


Figure 7.26: Transponder Database Import Dialog

Click the **[Yes]** button to continue. Otherwise, click the **[No]** button to abort. Be patient, as it may take a while, and watch for the disk activity to stop. If the data is imported successfully, a pop-up confirmation message appears. If the data is not imported successful, a pop-up error message appears. The error message will indicate the likely issue causing the import to fail.

7.14 Operator Database

The figure below is a typical screen from the **Operator Database**. The term operator is used to refer to a person with the authority to use the various features of the Security Escort system software. The term includes the Security department's dispatchers who initiate responses to alarms, Security Officers who may be required to produce incident reports, and other employees of the Security department who may be responsible for maintaining the **Subscriber** and **Operator Databases**.

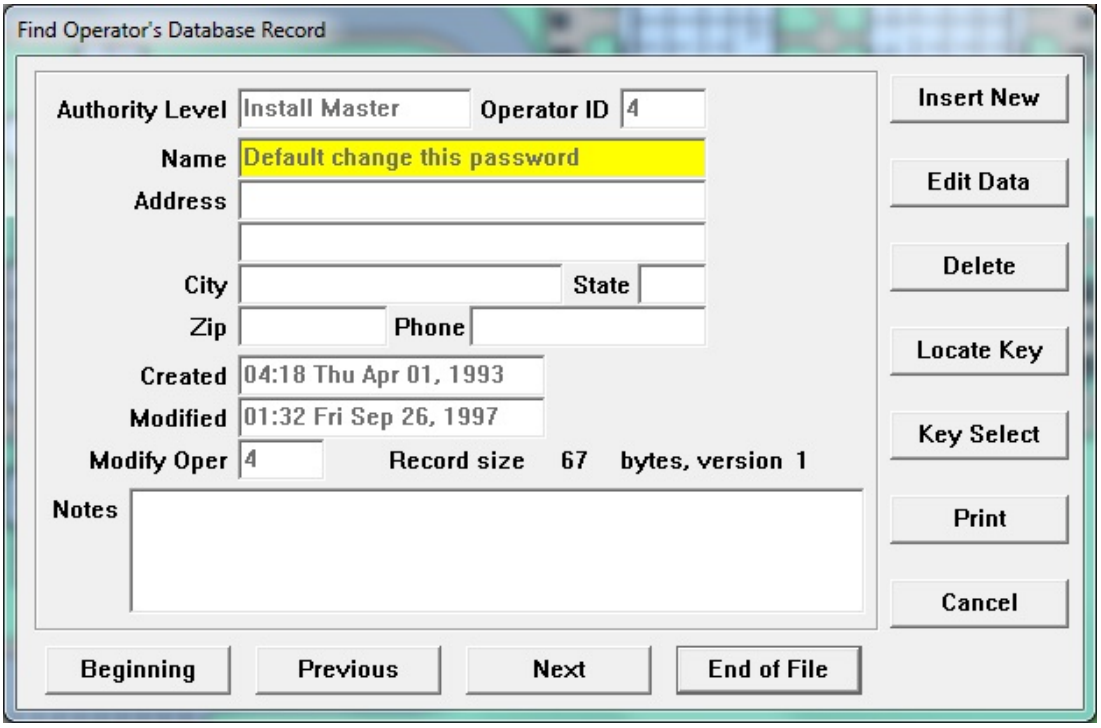


Figure 7.27: Find Operator's Database Record

The information in an **Operator Database** record includes the individual's password, full name, a unique operator identification number, an authority level, local address and phone number, and notes. All fields except the **Password** field are displayed. Even when a specific operator's file is edited (via the **[Edit Data]** button); the password is represented by a number of asterisks for security reasons.

7.14.1 Edit Operator Database record

When adding a new operator or editing the data for an existing operator, the **Edit Operator Record** dialog appears. Certain information fields must be completed to produce a valid record. The password, the authority level, and the name must be entered. All the other information in the operator's file is optional, including the local address, local phone number, and notes.

Notice!

There are two boxes for passwords in the **Edit Operator Record** dialog, **Password**, and **Password Verify**. Since the operator cannot see what is being entered while typing in the password field, it must be entered twice to safeguard against errors; password modifications are not accepted if the entries in the **Password** and **Password Verify** text boxes are not identical.

Figure 7.28: Edit Operator's Database Record

The **Operator ID** field will be automatically filled in with the next available ID number, there is no need to change the number selected.

7.14.2 Authority levels

An important consideration, when creating a new operator file, is the assignment of authority level. The authority level determines which functions an operator can perform on the system. Installing company representatives need access to almost every command in the Security Escort software; the key operator for the Security department usually requires access to alter the **Subscriber**, **Operator**, and **Report Databases** while a dispatcher may only need access to view these databases.

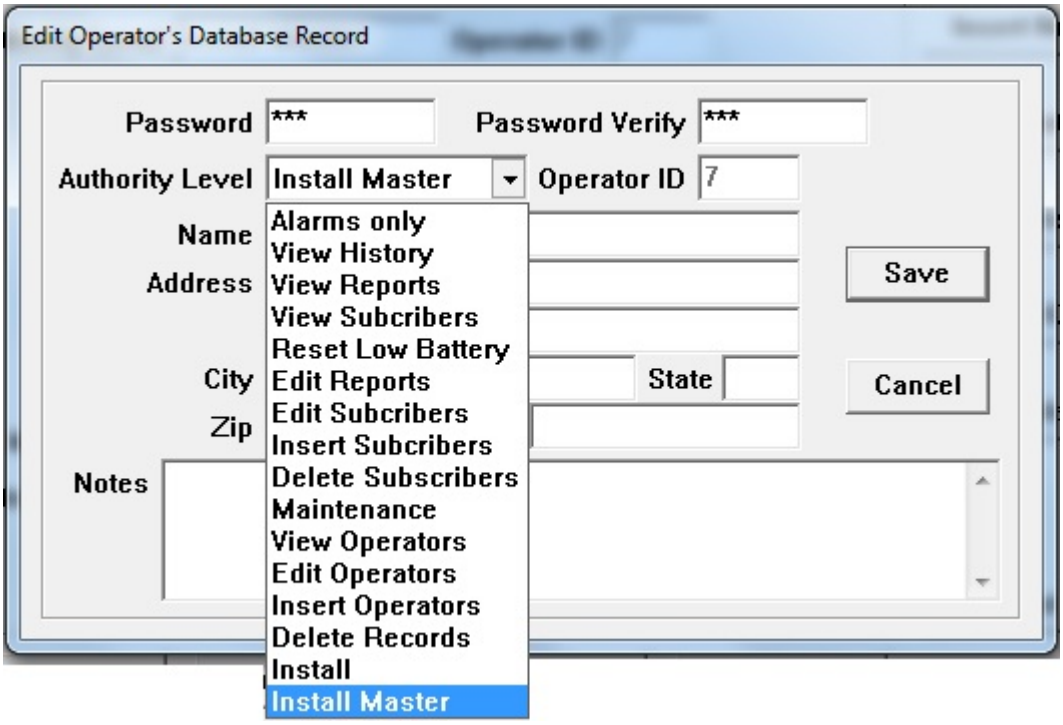


Figure 7.29: Edit Operator's Database Record

As a rule, any operator should be assigned the minimum authority necessary to carry out their task. The authority levels shown are in order with the highest authority shown on the bottom. Each authority level has the ability to perform all of the functions of the authorities shown above it.

7.15 Reports Database

The Security Escort software contains a report-generating feature that encourages prompt, uniform reporting of incidents. A sample of the alarm report dialog is shown in the figure below. The system software automatically captures the alarm data displayed on the alarm screen and enters it into a report form. The form also contains fields that describe the nature of the incident and the action taken. These fields are to be filled in by the responding officer.

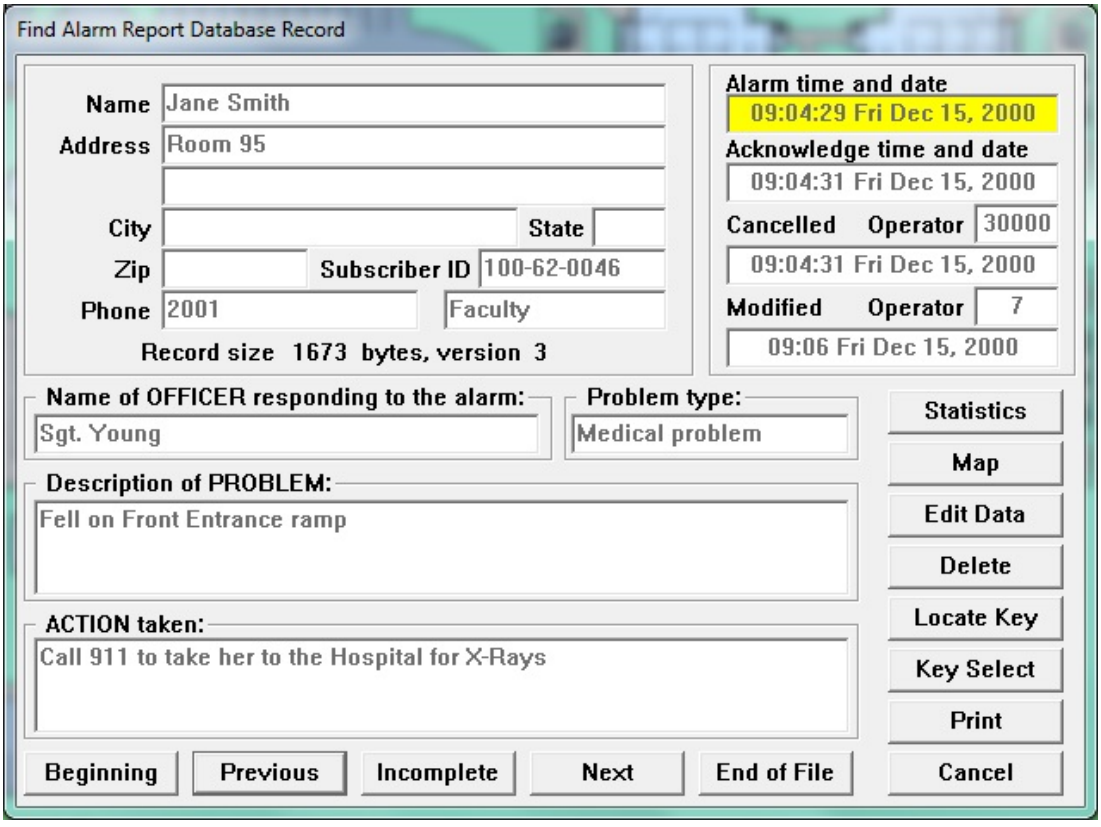


Figure 7.30: Find Alarm Report Database Record

The system software can be configured to require that a report be completed prior to the end of the shift in which the incident occurred. If the **Require Alarm Report** option is chosen in the **Edit Security Preferences** dialog, the report can be filled out immediately after the alarm is reset. However, if the report is not completed a reminder prompt appears on the screen every 5 min. for 30 min. before the end of the shift. The time at which the prompt is to display is also set in the **Edit Security Preferences** dialog.
All of the common database commands are available in the **Reports Database**, with the following additional commands.

7.15.1 Report statistics

Clicking the **[Statistics]** button summarizes all the alarm reports that are captured in the database. The alarm reports statistics window lists the number of alarms reports according to their problem types.

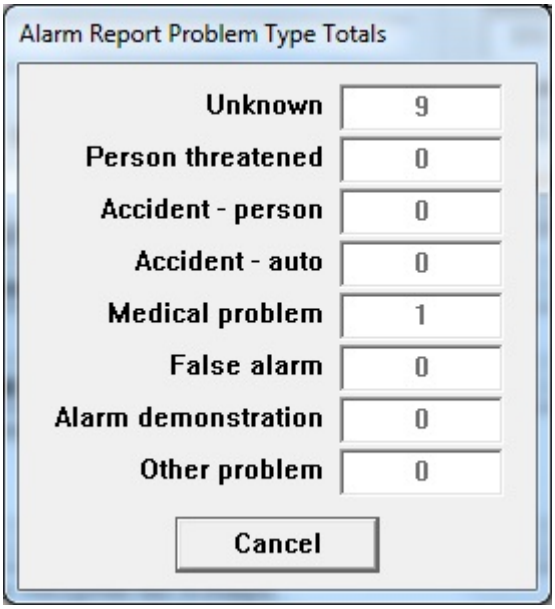


Figure 7.31: Alarm Report Statistics

7.15.2 Map

The act of resetting an alarm causes a report to be saved into the **Reports Database**. A part of the alarm report record is a copy of the alarm screen that is displayed at the time of the incident. Clicking the **[Map]** button reconstructs the screen as it appeared to the dispatcher.

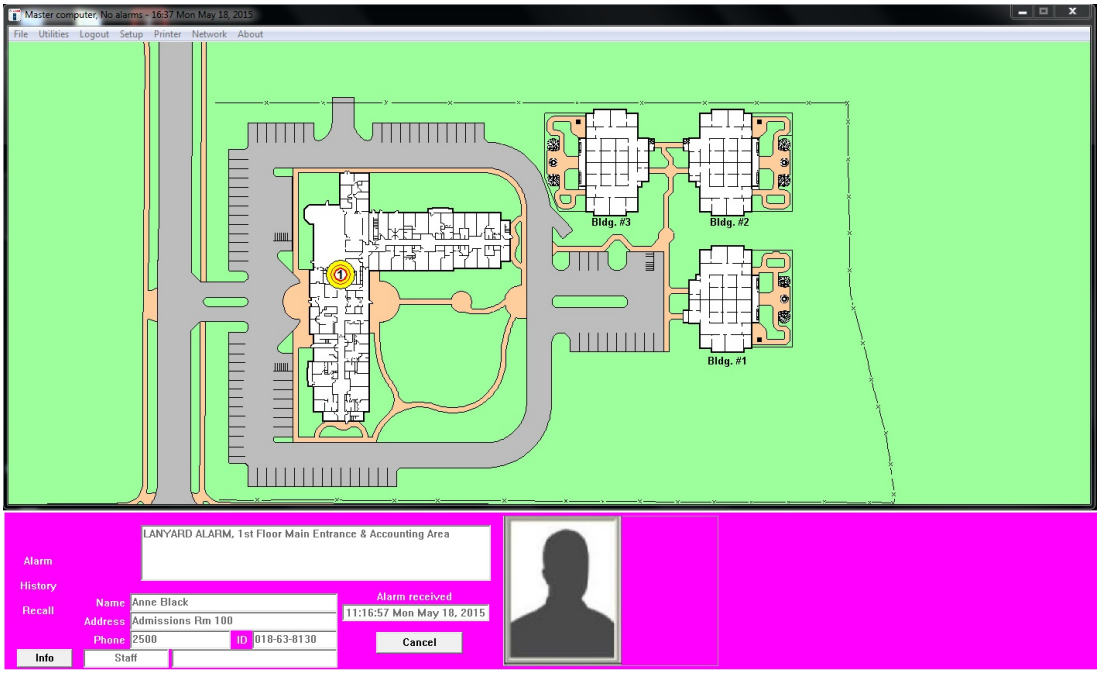


Figure 7.32: Active Alarm Map

7.15.3 Edit data

Select the appropriate problem type, and then enter the name of the officer who responded to the alarm. Finish with a description of the problem and the action taken. Save the updated record by clicking the **[Save]** button.

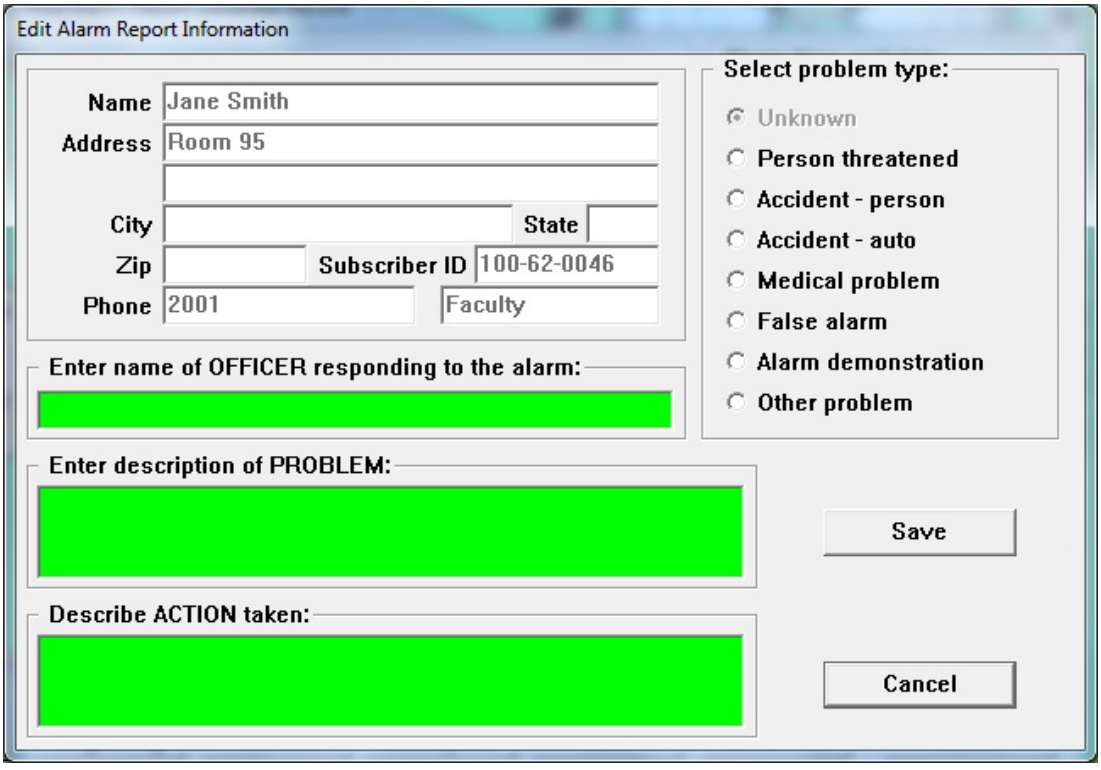


Figure 7.33: Edit Alarm Report Information

7.15.4 Delete

This button deletes the alarm report from the database. If the report is deleted, the data can not be recovered.

7.15.5 Locate Key

This button works similarly to the **[Locate Key]** button in the **Operator** and **Subscriber Database**. Entering the **Subscriber Name**, **Transmitter ID**, **Subscriber ID**, **Subscriber Class**, problem type, or a specific time and date can locate a specific report.

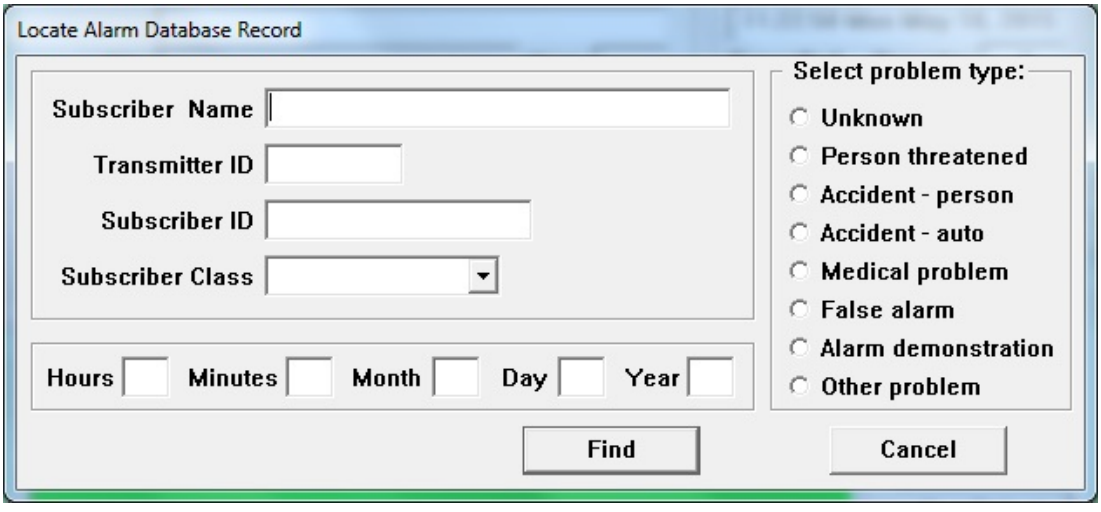


Figure 7.34: Locate Alarm Database Record

As in the **Operator** and **Subscriber Database**, the subscriber records are temporarily ordered according to the field entered in the **Locate Key** dialog.

7.15.6 Key Select

This button also works similarly to its counterparts in the **Operator** and **Subscriber Database**. Using it, the reports can be ordered by **Subscriber Name**, **Transmitter ID**, **Subscriber ID**, **Alarm Time**, **Problem Type**, or **Subscriber Type**.

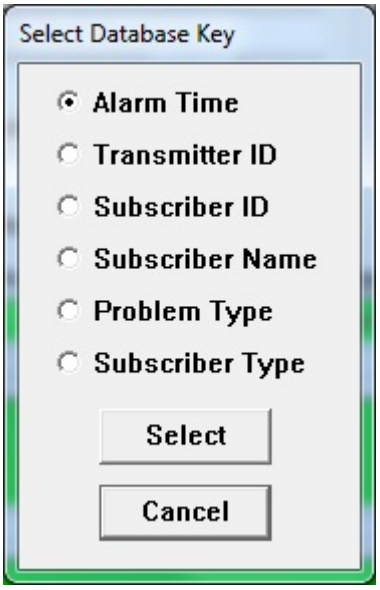


Figure 7.35: Select Database Key

7.15.7 Incomplete

When this button is clicked, the most recent incident report file that has not been completed will be displayed. The reports are not reordered when this command is used.

7.16 System redundancy

The Security Escort system redundancy is operational as long as master and slave controllers are configured in a network setup. By default, master computer is the one controlling the devices. If the master computer is unavailable for some reasons, slave computer could take over the operation (automatically or manually). Once the master computer is back online, slave computer will hand over the control to the master computer. If both the master and slave computers are not available, the system is not operational. Devices will take control by themselves.

Notice!

In the event where the master computer is unavailable and the slave computer takes control of the devices, alarms will be reported on the slave computer. If the master computer becomes available again, it will try to take control of the devices.
However, if there are still **unacknowledged alarms** on the slave computer, the master computer will not succeed in taking control, as the alarms need to be acknowledged on the slave computer first. The master computer will try to take control of the devices continuously until the unacknowledged alarms on the slave computer are acknowledged accordingly.
During the acknowledgement process, the receiver's sounders and red LEDs may not be turned off properly. You may need to turn these off manually from menu **Setup > Receiver configuration**.

There are 2 types of redundancy:

1. Automatic redundancy – system will automatically determine which computer will be the main controller based on the online availability of the master and slave computers (not applicable for RS232 connections).
2. Manual redundancy – manually determine which computer (master or slave) will be the main controller.

7.16.1 Automatic redundancy

Automatic redundancy kicks in during the following circumstances:

1. Master computer information is not configured in slave computer – If the master computer's related information is not configured in the slave computer, the slave computer will consider the master computer as unavailable. As such, the control of devices will switch to the slave computer automatically.
2. Master computer not reachable from slave computer – If the master computer's related information is configured in the slave computer, but the slave computer is unable to connect to the master computer, the slave computer will keep attempting to connect for 10 consecutive times. If the slave computer is still unable to connect to the master computer, the control of devices will switch to the slave computer automatically.
3. Master computer not responding – The slave computer will send "heart beat" messages to the master computer every second. The master computer will acknowledge each "heart beat" messages to the slave computer. If the slave computer did not receive 6 continuous "heart beat" acknowledgements from the master computer, the slave computer will consider the master computer as unreachable. As such, the control of devices will switch to the slave computer automatically.
4. Master computer acknowledges "heart beat" message – The slave computer will send the "heart beat messages" continuously. Once the slave computer receives the "heart beat" acknowledgement from the master computer, the slave computer will consider the master computer as being back in operation. As such, the slave computer disconnects all the devices and requests the master computer to take control of the devices.

7.16.2 Manual redundancy

Manual redundancy is only applicable to the following circumstances:

1. RS232 connected to either master or slave computer – Switch the RS232 connection manually to the other computer.
2. Newly RS232 connected computer takes control – The newly RS232 connected computer will inform the other computer to lose their control. The other computer will disconnect all the devices. The newly connected RS232 system will connect and take control of the devices.

8 System menus and dialogs

8.1 File menu

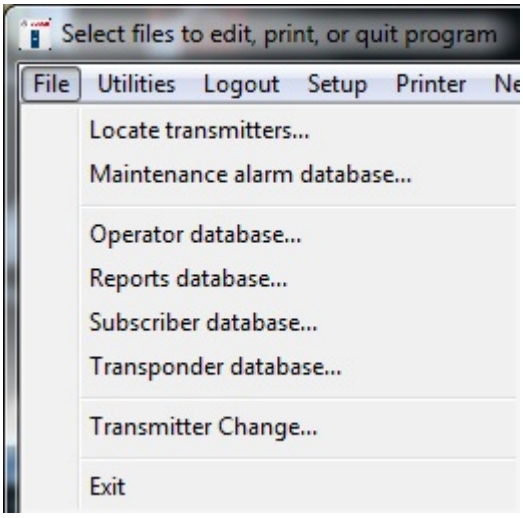


Figure 8.1: File Menu

8.1.1 Locate transmitters

This selection allows the operator to display the last reported location of the transmitter assigned to the indicated individual or asset. When the individual or asset is selected from the list, the time of the last supervision report is shown (or “None” is displayed if no supervision report was received from that transmitter). On the map, the last report location is shown.

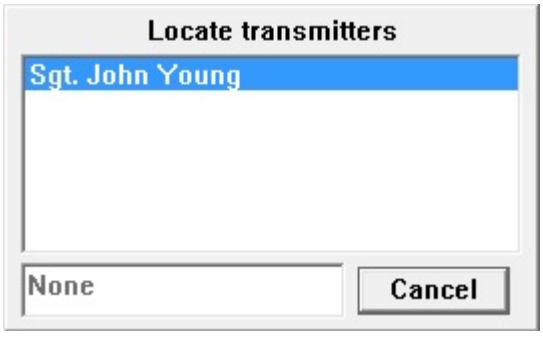


Figure 8.2: Locate Transmitters

8.1.2 Maintenance alarm database

Maintenance transmitters, when activated in the “Test” or “Alarm” mode, generate a series of multiple data packets like subscriber transmitters. However, a special code in each packet identifies the transmitter as a “Maintenance Transmitter”.
The receiver responds to a maintenance “Alarm” or “Test” transmission in the same way it responds to a subscriber “Alarm” or “Test”, unless the receiver has been put in the “Setup” mode. The transponder then reports the maintenance transmitter identification number and all signal levels to the Central Console, which then creates the location estimate and processes the data as it would for a normal alarm.

Notice!
All maintenance transmitters are assumed to be valid so there is no need for the Central Console to check for the identification number in the Subscriber Database.

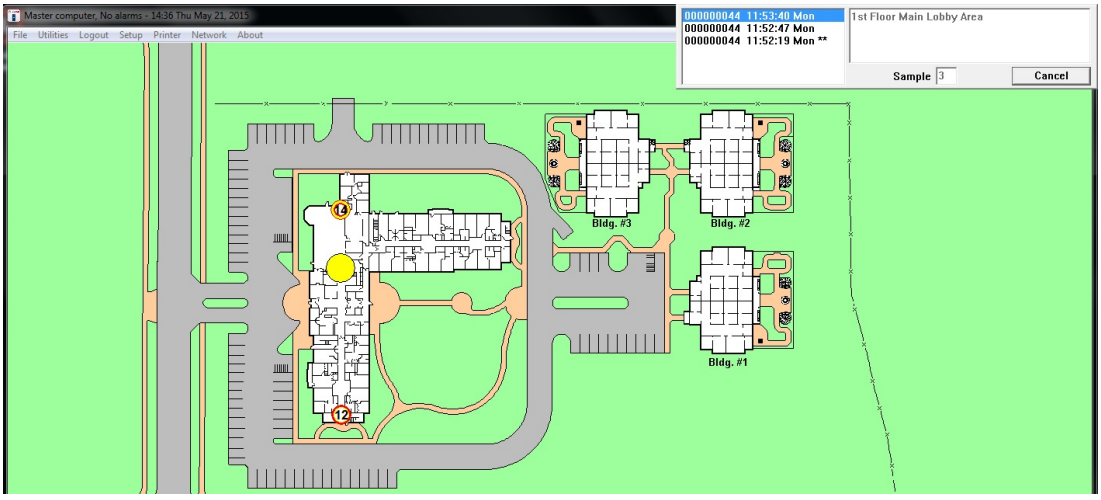


Figure 8.3: Maintenance "Alarm" With Signal Levels Shown in Icons

"The Central Console will not generate an audible alert for the operator, nor will it create an “alarm” display on the main Central Console screen. Because they can be set to graphically display received signal levels, maintenance “alarms” are very useful to verify that the system coverage exists at any location in the protected area, and that receiver redundancy is adequate.

8.1.3 Transmitter Change

The **Transmitter Change** command on the **File** menu is used when it is necessary to change a subscriber’s transmitter.
Selecting **Transmitter Change** opens the **Locate Subscriber’s Database Record** dialog. The subscriber’s record in the **Subscriber Database** can be quickly found by entering the **Subscriber Name**, **Subscriber ID**, current **Transmitter ID**, **Address Items**, **Phone Number**, **Pager Items** or **Pager Group**. This method of locating a particular subscriber’s record is identical to using the **[Locate Key]** button in the **Subscriber Database**: the first record, which is identical to the entered data, is shown. It may be necessary to scroll using the **[Previous]** and **[Next]** buttons to find the appropriate record.

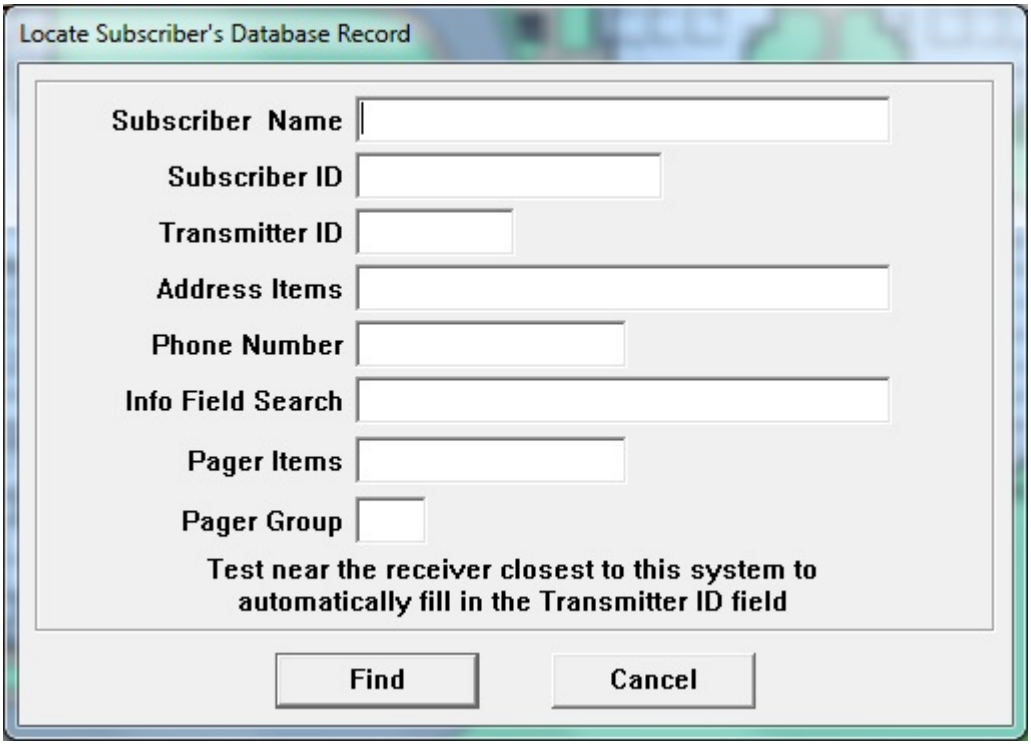


Figure 8.4: Locate Subscriber's Database Record

Perform a test using the old transmitter if possible. This should fill in the **Transmitter ID** field. Then click the **[Find]** button.

Notice!

Be absolutely certain that the correct record is displayed before entering the new **Transmitter ID** (Identification Code). Changing the wrong subscriber's record makes two records ineffective: the correct subscriber will be misidentified and the subscriber whose record was incorrectly altered will be disabled. If possible, perform a test with the subscriber's old transmitter after the change has been made: the test should fail.

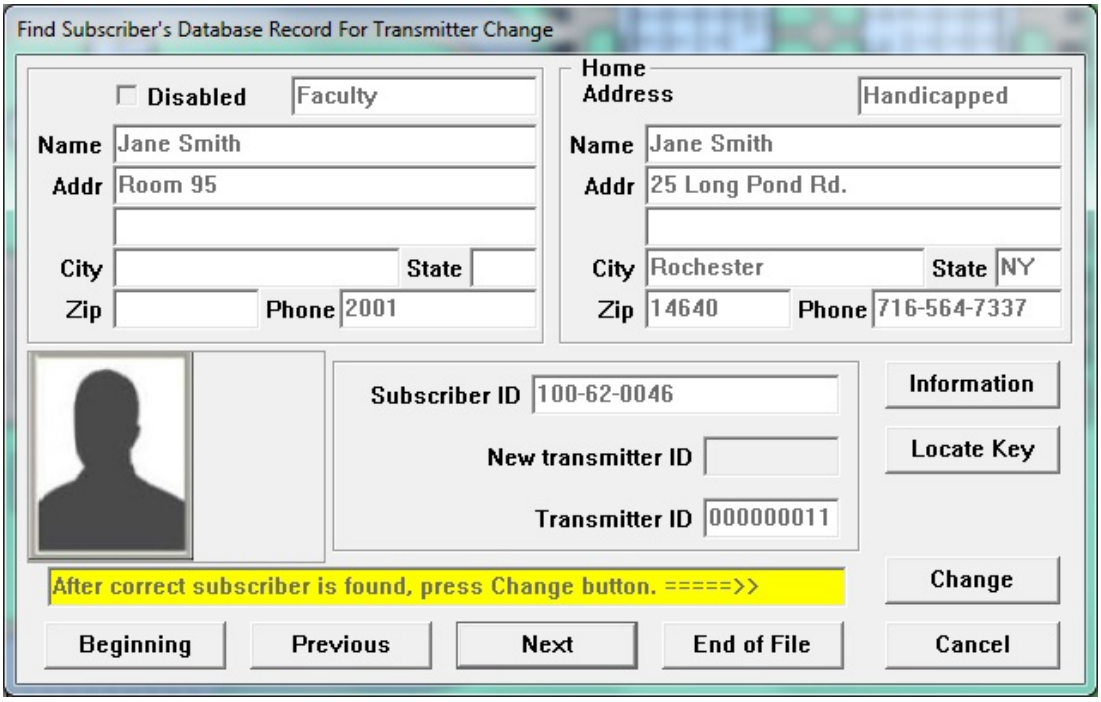


Figure 8.5: Find Subscriber's Database Record

When the correct subscriber's record is displayed, click on the **[Change]** button and perform a test using the new transmitter. The new transmitter identification code will be automatically populated into the **New transmitter ID** field.

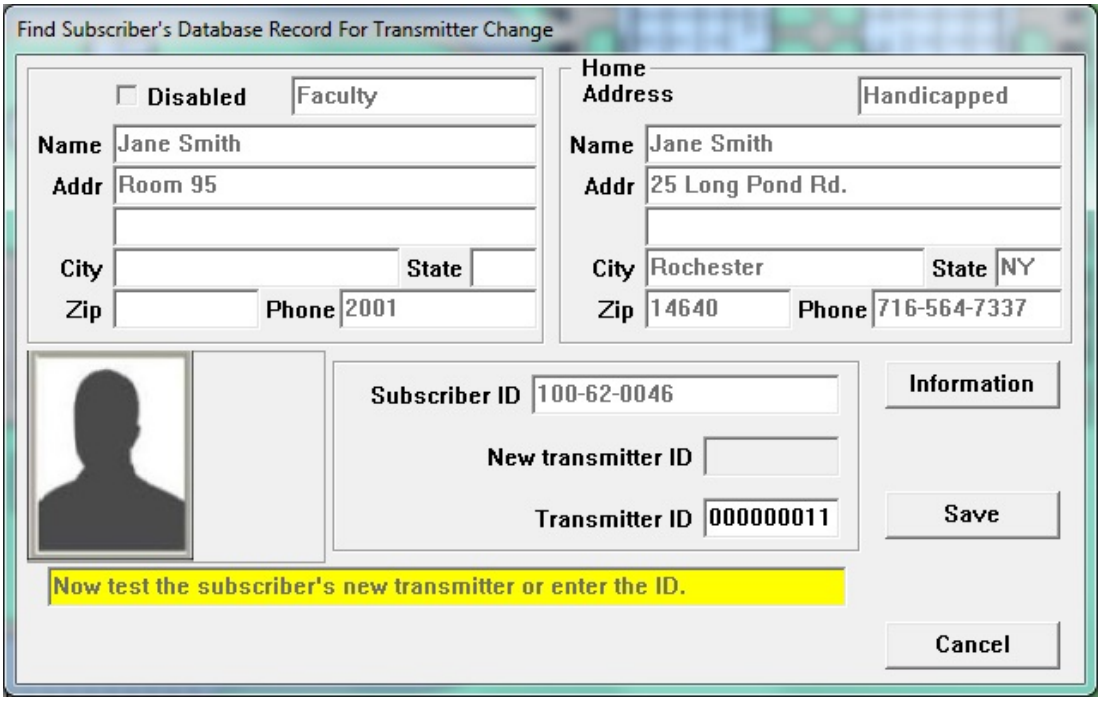


Figure 8.6: Save Subscriber's Database Record after Change of Transmitter ID

Manually enter the **New transmitter ID** into the **Transmitter ID** field or use the mouse to highlight the old **Transmitter ID** value, press and hold the <Shift> key and tap the <Insert> key. Then click the **[Save]** button. A prompt appears, asking for a second test to confirm the change.
Test the new transmitter again. You should see a green light on a nearby receiver, and this dialog should automatically disappear from the screen, confirming the change was successful.

8.2 Utilities menu

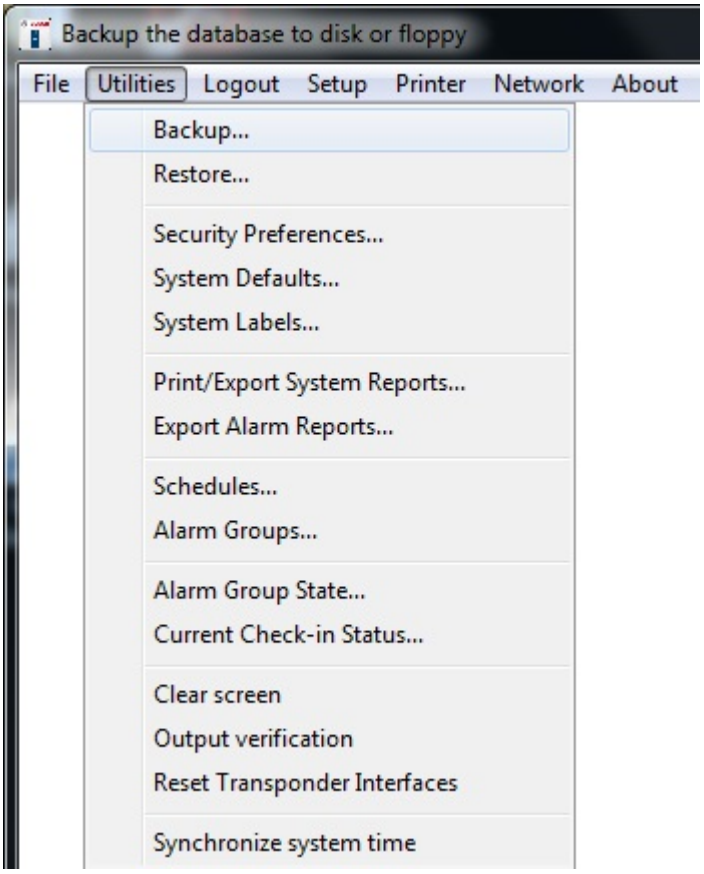


Figure 8.7: Utilities Menu

8.2.1 Backup dialog

This feature provides a convenient process for saving the information in the databases to backup files.

Warning!
To prevent the accidental loss, the databases should be backed up at least once a week to multiple backups. At least one of these backup copies should be kept in a different location from the central console's location.

Weekly backups are recommended to permit data recovery if the computer memory should become corrupted. If this unlikely event occurs, an operator can quickly restore the databases in question with the **Restore** command. Backups should be made any time significant changes are made to any database.

Notice!

If the Security Escort system is configured to share the database, you will need to exit the Security Escort program on all slave and workstation computers. The master computer will not be able to perform the backup properly as other computers are also using the files. The master computer needs to have exclusive use of the database files.

Figure 8.8: Backup Dialog

When the **Backup** menu item is chosen, options are presented to save the databases to the master or slave computer's hard drive, a cartridge drive, or to a floppy drive of this computer. When saving to a floppy disk or cartridge drive, verify that the appropriate disk or cartridge is inserted into the drive before clicking the **[Backup]** button. To abort the process, click the **[Cancel]** button in the dialog.

Only the databases with a checkmark will be backed up. Typically all databases should be backed up at once. Only when they do not fit on one floppy disk should you save individual databases to one floppy, then switch floppy disks and repeat the procedure to save the rest of the files. As insurance against database problems, multiple backups to different disks should be made frequently. At least one backup copy should be stored in a different location from this system (remember to keep this copy current).

Operators	This is the database of all of the individuals with passwords to operate the system software and acknowledge alarms.
Subscriber	This database contains all of transmitters assigned in the system.
Transponders	This database contains the configuration of the transponders, receivers, virtual receivers and alert units.
Reports	This database contains all of the alarm reports and related alarm map screens.
Master Database drive	Store the backup files in the Security Escort Master Database path. See the **System Directories and Network Address** dialog.

Slave Database drive	Store the backup files in the Security Escort Slave Database path. See the **System Directories and Network Address** dialog.
Local Escort drive	Store the backup files in the save sub-directory as the Security Escort System components are stored on this computer (typically C:\ESCORT).
Cartridge disk drive	Store the backup files in the **Backup / restore to disk cartridge path** assigned in the **System Preferences** dialog. This path may point to a cartridge disk drive, to a local hard disk or to a network disk drive.
Floppy A:	Store the backup files on the floppy disk in floppy disk drive A.
[Backup]	When the **[Backup]** button is clicked, all databases selected with a checkmark will be saved to the destination selected on the right.

8.2.2 Restore dialog

Should one or more database files become corrupted or erased due to a hard drive failure, power surges or other unpredictable events, it is necessary to restore the databases from backup files. The **Restore** function allows loading of selected databases from backup files. It is not necessary to perform the **Restore** function on all databases in order to restore any one. All changes that occurred since the last backup are lost when a database is restored. Therefore, restore only those databases with a problem. Backups should be made whenever significant changes are made to any database.

Notice!

If the Security Escort system is configured to share the database, you will need to exit the Security Escort program on all slave and workstation computers. The master computer will not be able to perform the restore properly as other computers are also using the files. The master computer needs to have exclusive use of the database files.

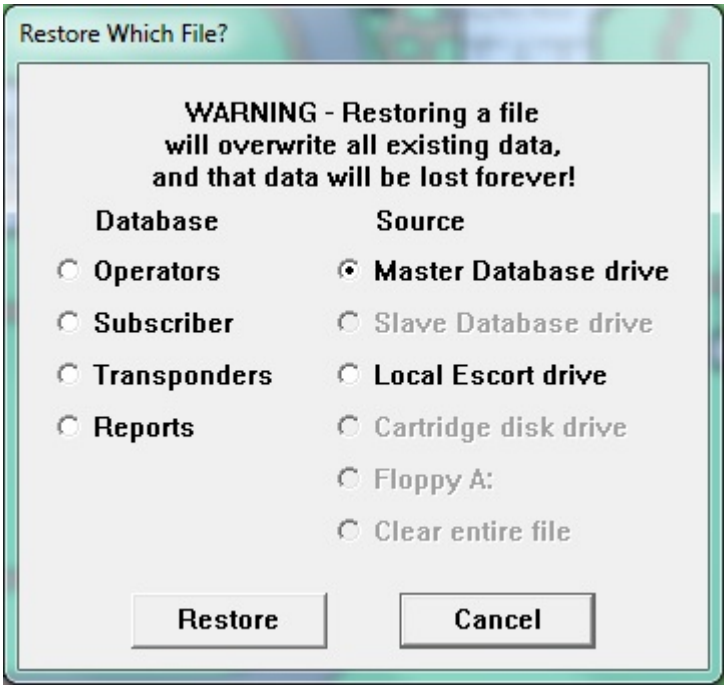


Figure 8.9: Restore Dialog

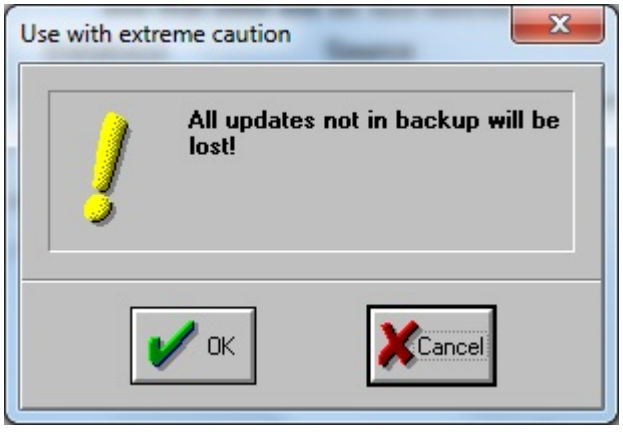
Select the database to be restored on the left. On the right, this is where the database backup is currently located. Click the **[Restore]** button to replace the existing database file with the backup. This process also rebuilds the database and its index tables to correct most database structure problems. To abort the restore process, click the **[Cancel]** button.

Operators	This is the database of all of the individuals with passwords to operate the system software and acknowledge alarms.
Subscriber	This database contains all of transmitters assigned in the system.
Transponders	This database contains the configuration of the transponders, receivers, virtual receivers and alert units.
Reports	This database contains all of the alarm reports and related alarm map screens.
Master Database drive	Store the backup files in the Security Escort **Master Databasepath**. See the **System Directories and Network Address** dialog.
Slave Database drive	Store the backup files in the Security Escort **Slave Databasepath**. See the **System Directories and Network Address** dialog.
Local Escort drive	Store the backup files in the save sub-directory as the Security Escort System components are stored on this computer (typically “C:\ESCORT”).
Cartridge disk drive	Store the backup files in the Backup / restore to disk cartridge path assigned in the **System Preferences** dialog. This path may point to a cartridge disk drive, to a local hard disk or to a network disk drive.

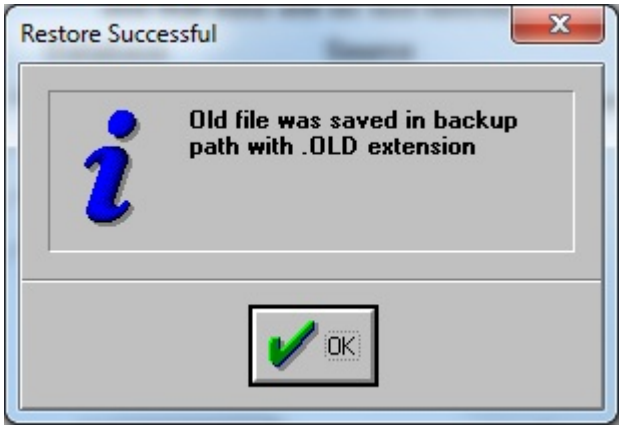
Floppy A Store the backup files on the floppy disk in floppy disk drive A.

Clear entire file If selected and the **[Restore]** button clicked, then that entire database will be cleared of all records. This selection must be used with extreme caution! Hold down the <Shift>+<Ctr;> keys when opening the dialog to enable the **Clear entire file** option.

[Restore] When the **[Restore]** button is clicked the database selected will be restored from the destination selected on the right.



This message box is a reminder that if changes to the system databases have been made since the backup was made, the changes will be lost. Therefore those changes must be redone to the restored database.



This message box indicates the restore has been completed. The previous database file has been renamed with an .OLD extension and saved in the Escort sub-directory. Only the most recent database of each type is retained.

8.2.3 Print/Export System Reports

This dialog allows the system reports to be printed on demand, scheduled for printing each night at midnight or weekly on Sunday at midnight. To print a report, select the left-checkbox for each desired report and click the **[Print]** button. Select the **Midnight report** or the **Sunday only** checkboxes to automatically schedule the selected report at those times.

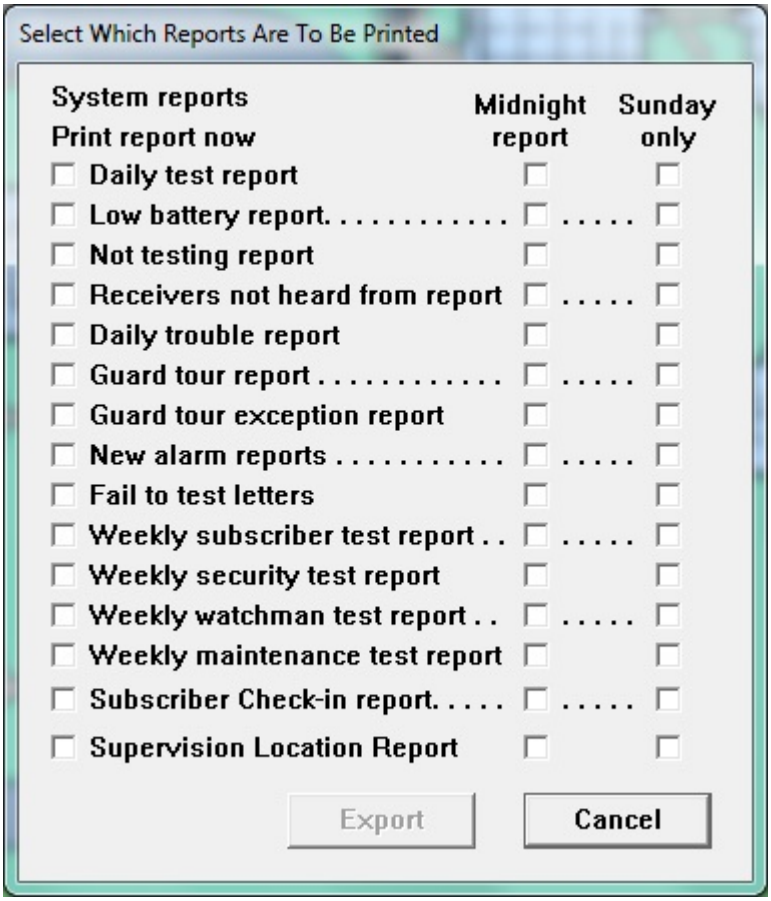


Figure 8.10: Print/Export System Reports Dialog

Daily test report	Report of testing by classes of subscriber for the last 24 hours broken down by hour.
Low battery report	Report of all subscriber transmitters currently reporting low battery.
Not testing report	Report of all subscriber transmitters that have not tested their transmitters within the last 28 days.
Receivers not heard from report	Report of all receivers that have not heard transmissions recently. This could indicate a problem with the receiver's ability to hear alarms and test transmissions.
Daily trouble report	Report of all the troubles currently being reported by transponders, receivers and alert units.
Guard tour report	Report of the guard tours collected within the last day. This selection does not generate a printed report. However, the **Midnight report** and **Sunday only** checkboxes must be checked to write a file of the guard tour information. Another application like Microsoft Excel can sort and print the desired reports.
Guard tour exception report	The guard tour exception reports collected within the last day. Not currently implemented.
New alarm reports	Alarm reports for all of the new alarms that have been received by the system.

Fail to test letters	Notices to all of the subscribers that have not tested within the last 28 days. Not currently implemented.
Weekly subscriber test report	Report of subscriber testing for the last 7 days broken down by hour.
Weekly security test report	Report of security personnel testing for the last 7 days broken down by hour.
Weekly watchman test report	Report of watchman personnel testing for the last 7 days broken down by hour.
Weekly maintenance test report	Report of maintenance testing for the last 7 days broken down by hour.
Subscriber Check-in report	Report of all subscribers that failed to check-in during the last scheduled check-in period.
Supervision Location report	Report of all supervision enabled subscribers and their last known location.
[Print]	Clicking this button prints all reports that are checked in the left-hand check boxes.
[Export]	Clicking this button exports all reports that are checked in the left-hand checkboxes.
Print report now	Reports that are selected are printed when the **Print** button is clicked.
Midnight report	Reports are automatically generated every midnight for all reports that are checked in the **Midnight report** checkboxes.
Sunday report	Reports are automatically generated every Sunday at midnight for all reports that are checked in the **Sunday report** checkboxes.

8.2.4 Export Alarm Reports

This dialog allows the alarm reports to be exported to CSV file. To export an alarm report, you may directly enter the alarm date range, or click the **[...]** (ellipsis) button in **From Date**, **To Date** fields and select **From Time**, **To Time** from the respective drop-down values. An alarm report can also be generated based on the subscriber details. Select the **Subscriber ID**, **Subscriber Name**, **Transmitter ID** or **Subscriber Type** from the drop down list to generate an alarm report only for the selected values.

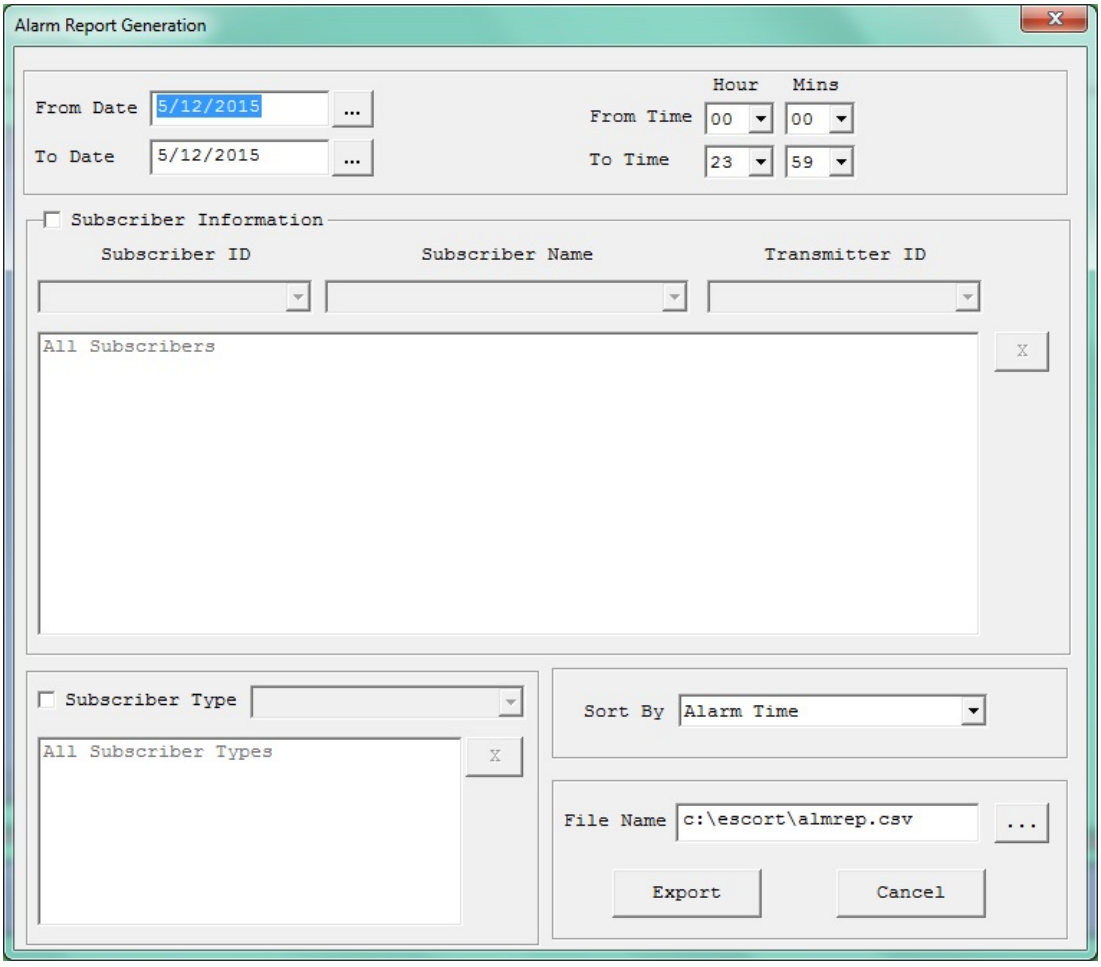


Figure 8.11: Export Alarm Report

The alarm report can be sorted by **Alarm Time**, **Transmitter ID**, **Subscriber Name**, **Problem Type**, **Subscriber Type**, by using the **Sort By** drop-down list. You can change the report name and file location by pressing the **[...]** (ellipsis) button. Clicking the **[Export]** button saves the report to the specified file. Clicking the **[Cancel]** button cancels the report generation and exits from the dialog window.

8.2.5 Clear Screen

To clear the screen of any outdated or unwanted data, choose this feature from the **Utilities** menu. The screen automatically resets to its normal operations mode.

8.2.6 Output verification

When selected, the system is scanned to verify that all alarm outputs are in the correct state. Any output found in the wrong state is corrected.

8.2.7 Synchronize System Time

Selecting this option on the master computer causes the time on the slave and all of the workstation computers to be updated to the master computer's time.

8.3 Setup commands

8.3.1 Show History

When selected, the default map display is replaced by a scrolling text window showing the most recent events that occurred in the system. The window can list historical events and operations of the Central Console software. Examples include list of any alarms and the actions taken, name of person who logged into the Central Console, changes to the database, communication results between the devices, and so on.
The events displayed can be selected in the **History Filter** dialog under the **Setup** Menu. After **Show History** is selected, this menu item changes to **Show Map**.

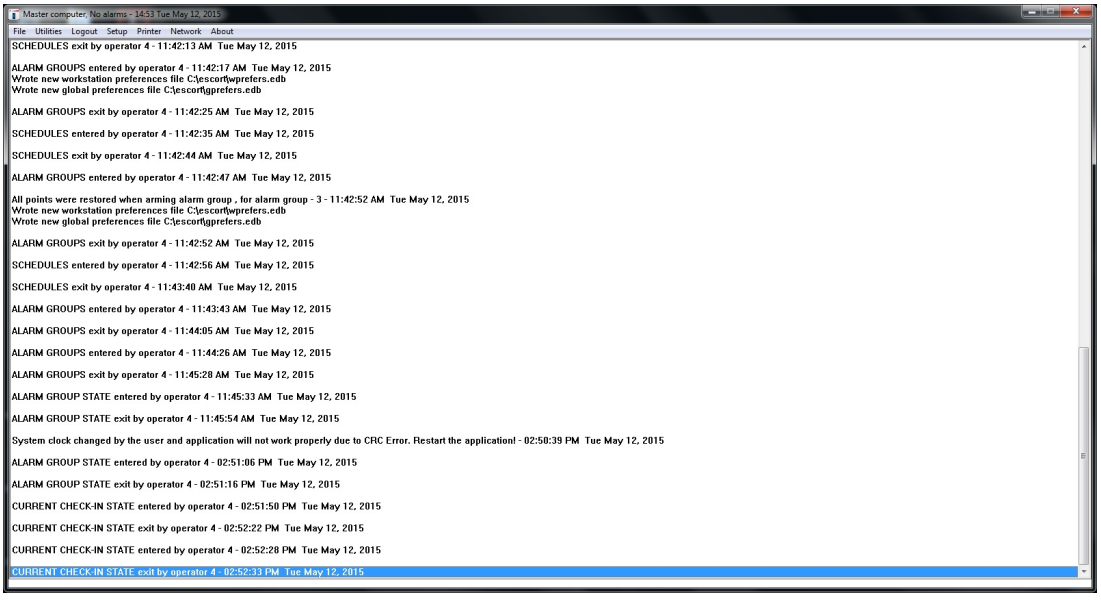

Master computer No alarms - 14:53 Tue May 12, 2015
File Utilities Logout Setup Printer Network About
SCHEDULES exit by operator 4 - 11:42:13 AM Tue May 12, 2015
ALARM GROUPS entered by operator 4 - 11:42:17 AM Tue May 12, 2015
Wrote new workstation preferences file C:\escort\wprefers.edb
Wrote new global preferences file C:\escort\gprefers.edb
ALARM GROUPS exit by operator 4 - 11:42:25 AM Tue May 12, 2015
SCHEDULES entered by operator 4 - 11:42:35 AM Tue May 12, 2015
SCHEDULES exit by operator 4 - 11:42:44 AM Tue May 12, 2015
ALARM GROUPS entered by operator 4 - 11:42:47 AM Tue May 12, 2015
All points were restored when arming alarm group , for alarm group - 3 - 11:42:52 AM Tue May 12, 2015
Wrote new workstation preferences file C:\escort\wprefers.edb
Wrote new global preferences file C:\escort\gprefers.edb
ALARM GROUPS exit by operator 4 - 11:42:52 AM Tue May 12, 2015
SCHEDULES entered by operator 4 - 11:42:56 AM Tue May 12, 2015
SCHEDULES exit by operator 4 - 11:43:40 AM Tue May 12, 2015
ALARM GROUPS entered by operator 4 - 11:43:43 AM Tue May 12, 2015
ALARM GROUPS exit by operator 4 - 11:44:05 AM Tue May 12, 2015
ALARM GROUPS entered by operator 4 - 11:44:26 AM Tue May 12, 2015
ALARM GROUPS exit by operator 4 - 11:45:28 AM Tue May 12, 2015
ALARM GROUP STATE entered by operator 4 - 11:45:33 AM Tue May 12, 2015
ALARM GROUP STATE exit by operator 4 - 11:45:54 AM Tue May 12, 2015
System clock changed by the user and application will not work properly due to CRC Error. Restart the application! - 02:50:39 PM Tue May 12, 2015
ALARM GROUP STATE entered by operator 4 - 02:51:06 PM Tue May 12, 2015
ALARM GROUP STATE exit by operator 4 - 02:51:16 PM Tue May 12, 2015
CURRENT CHECK-IN STATE entered by operator 4 - 02:51:50 PM Tue May 12, 2015
CURRENT CHECK-IN STATE exit by operator 4 - 02:52:22 PM Tue May 12, 2015
CURRENT CHECK-IN STATE entered by operator 4 - 02:52:28 PM Tue May 12, 2015
CURRENT CHECK-IN STATE exit by operator 4 - 02:52:33 PM Tue May 12, 2015

Figure 8.12: Show History Log

8.3.2 History Filter Dialog

This dialog selects the classes of events recorded for (sent to) specific output devices. From the **Select Destination** group, select the **History screen**, **Printer**, **History files** or **System serial ports** option. Notice that when this selection is changed, the checked items also change. There is a different set of events output for each destination selected. For each destination, the events must be individually configured.

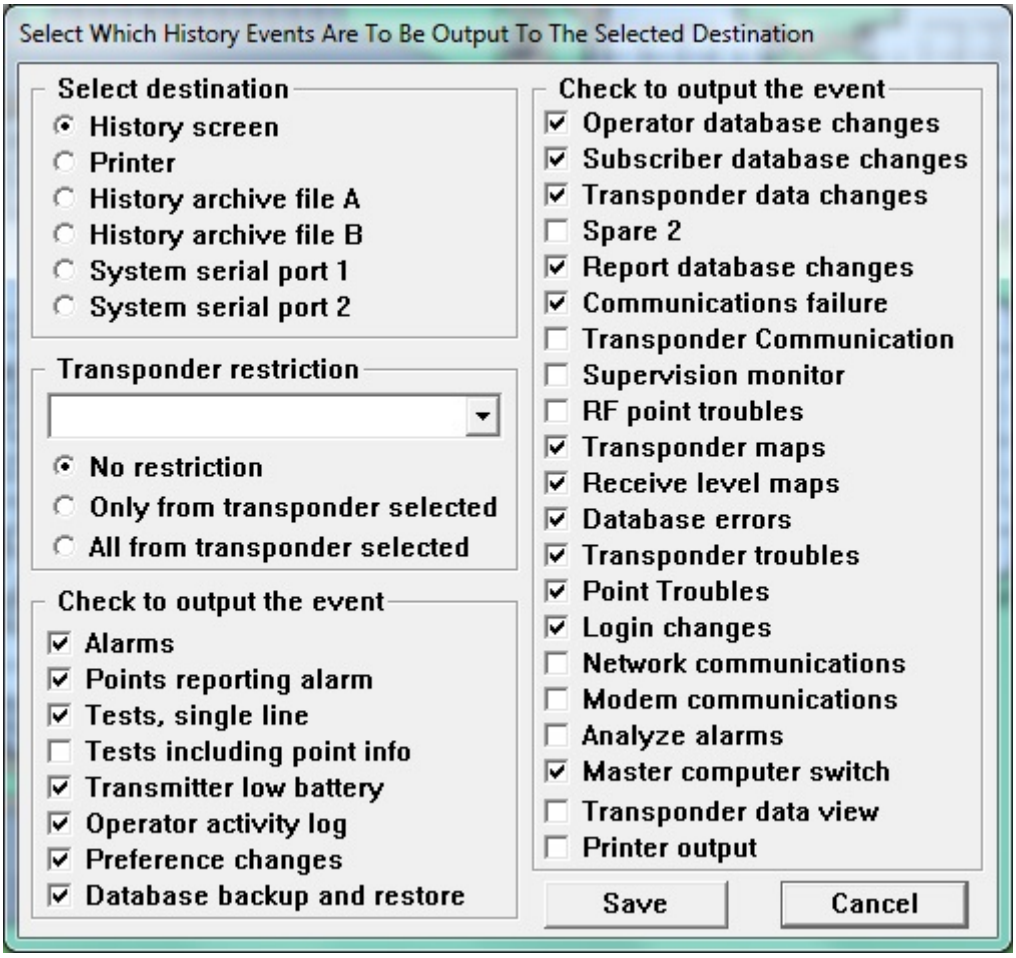


Figure 8.13: History Filter Dialog

History screen	This option selects the events to be displayed on the computer screen when **Show History** is selected.
Printer	This option selects the events to be sent to the printer.
History archive file A	This option selects the events to be sent to the a_audit.txt file stored in the Security Escort sub-directory (typically C:\ESCORT \a_audit.txt). There is a minimum set of events that cannot be disabled, so they are always recorded.
History archive file B	This option selects the events to be sent to the b_audit.txt file stored in the Security Escort sub-directory (typically C:\ESCORT \b_audit.txt).
System serial port 1	This option selects the events to be sent to the system serial port 1. System serial port 1 is assigned a physical comm port in the **Remote Comm Port Setup** dialog, and the **History Filter Output** field must be set in the **Remote Setup** dialog.
System serial port 2	This option selects the events to be sent to the system serial port 2. System serial port 2 is assigned a physical comm port in the **Remote Comm Port Setup** dialog, and the **History Filter Output** field must be set in the **Remote Setup** dialog.

Transponder restriction	This option selects a transponder for the following restrictions: **No Restriction:** This selection is typically left at this setting at all times. The output is not restricted by an individual transponder. **Only From Transponder Selected:** The selected events are only output if they were reported from the transponder selected in the transponder above. **All from Transponder Selected :** All events are reported from the transponder selected above. The selected events are reported from all other transponders in the system.
Alarms	Outputs the information about an alarm including location, but not the transponder and receiver levels. This is the data typically sent to a printer.
Points, reporting alarm	Outputs the transponder and receiver levels for an alarm. Typically, this is the data too detailed to send to a printer and is used for diagnostics, not normal system operation.
Tests, single line	Outputs the simple information about a test. Typically, this is the data normally sent to a printer.
Tests including point Info	Outputs the transponder and receiver levels for a test. This is the data usually too detailed to send to a printer and is used for diagnostics, not normal system operation. If this option is selected, **Test, single line** above, would not be selected for the same output device.
Transmitter low battery	Outputs low battery reports received from transmitters.
Operator activity log	Outputs all other operator activity (audit trail) not covered by specific event selections.
Preferences changes	Outputs all changes made to system preference selections.
Database backup and restore	Records all database backup and restore activity.
Operator database changes	Records all changes to the operator database.
Subscriber database changes	Records all changes to the subscriber database.
Transponder data changes	Records all changes to the transponder database.
Spare 2	This is a future option that has no function at this time (leave unchecked).
Report database changes	Records all changes to the **Alarm Report Database**.
Communications failure	Records all communication failures and restorations.
Transponder communication	Records all communications to transponders. This selection is only used for engineering diagnostics. Leaving this item selected generates a significant amount of history and fills up the hard disk drive quickly. Leave this item unchecked.
Supervision monitor	Reports changes in the supervision status for all transmitters that are being supervised.
RF point troubles	Output all reported radio frequency communication of receiver and alert unit troubles. Typically this item would be checked for devices used to monitor problems.

Transponder maps	Outputs all transponder status maps. This selection is only used for diagnostics. Leave this item unchecked.
Receive level maps	Outputs all maintenance alarm receive level maps. This selection is only used for diagnostics. Leave this item unchecked.
Database errors	Outputs all reported database errors. This item is checked.
Transponder troubles	Outputs all reported transponder troubles. This item is checked for devices used to monitor problems.
Point troubles	Outputs all reported receiver and alert unit troubles. This item is checked for devices used to monitor problems.
Login changes	Reports all new system operator login and logout activity.
Network communications	Records all communications between networked computers. This selection is only used for engineering diagnostics. Leaving this item selected, generates a significant amount of history and fills up the hard disk drive very quickly and may bog down the system during high traffic times. Always leave this item unchecked.
Modem communications	Records all communications to the modem for remote communications and pager access. This selection is only used for diagnosing pager communication problems. Leave this item unchecked.
Analyze alarms	This option outputs data allowing an engineer to evaluate how well the location algorithm is performing. Leave this item unchecked.
Master computer switch	Records when the master and slave computers switch roles.
Transponder data view	Allows the data created by the **Transponder Data View** screen to be output. This selection is only used for engineering diagnostics. Leave this item unchecked.
Printer output	Allows the data being sent to the printer to be sent to other outputs. This item is unchecked.

8.3.3 Popup Trouble Filter

The Security Escort System contains many built-in self testing features. Each transponder tests the condition of the receivers and alert units connected to it.

When the transponder finds a device reporting a trouble condition, it communicates the problem and the device identity to the Central Console. This generates a brief alert tone, displays a pop-up message for the operator, and sends an optional pager message. The message indicates the nature of the trouble and instructs the operator on the proper course of action. The event is recorded on the hard disks of both the main and backup computers and on the printout.

The status of the device is recorded in the **Transponder Current Status** menu item under the **Setup** menu.

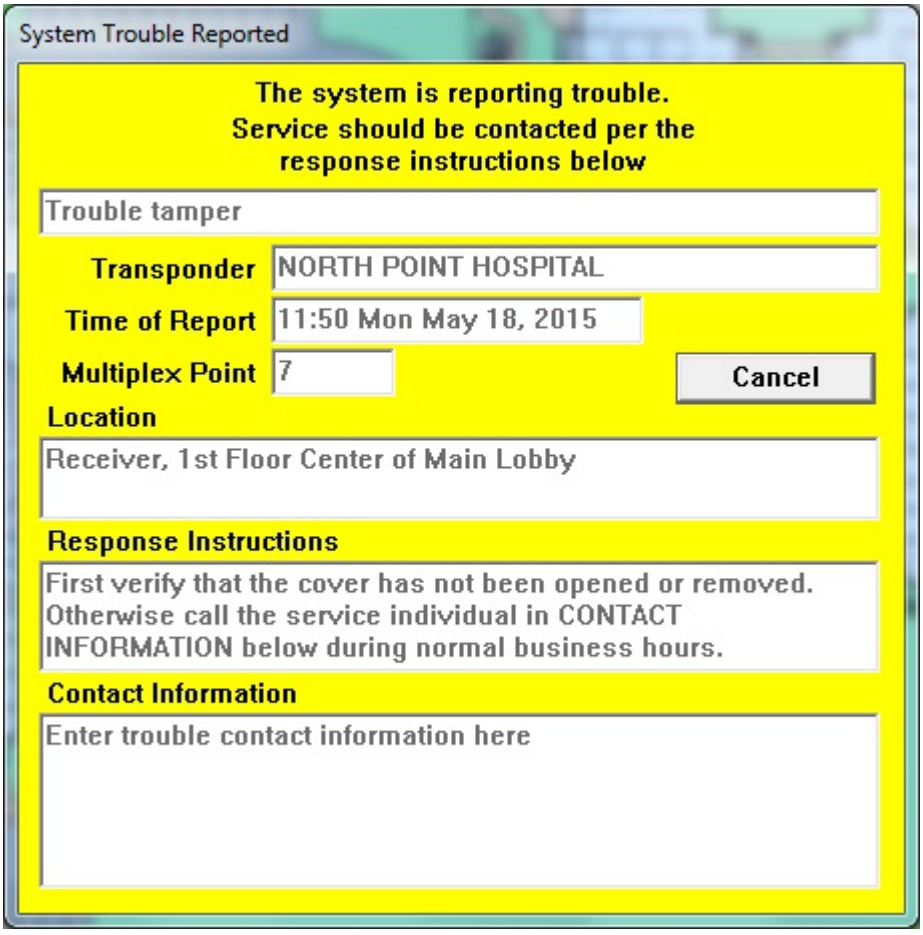


Figure 8.14: "Pop-Up" Alert Showing Tamper Trouble

This dialog allows the selection of which type of troubles that will appear in pop-up messages on the console screen, or be sent to the service pager. The troubles described below are always recorded in the **Transponder current status** window, but may or may not produce a pop-up display or pager message, depending on the selections for **Popup** or **Pager** checkboxes.

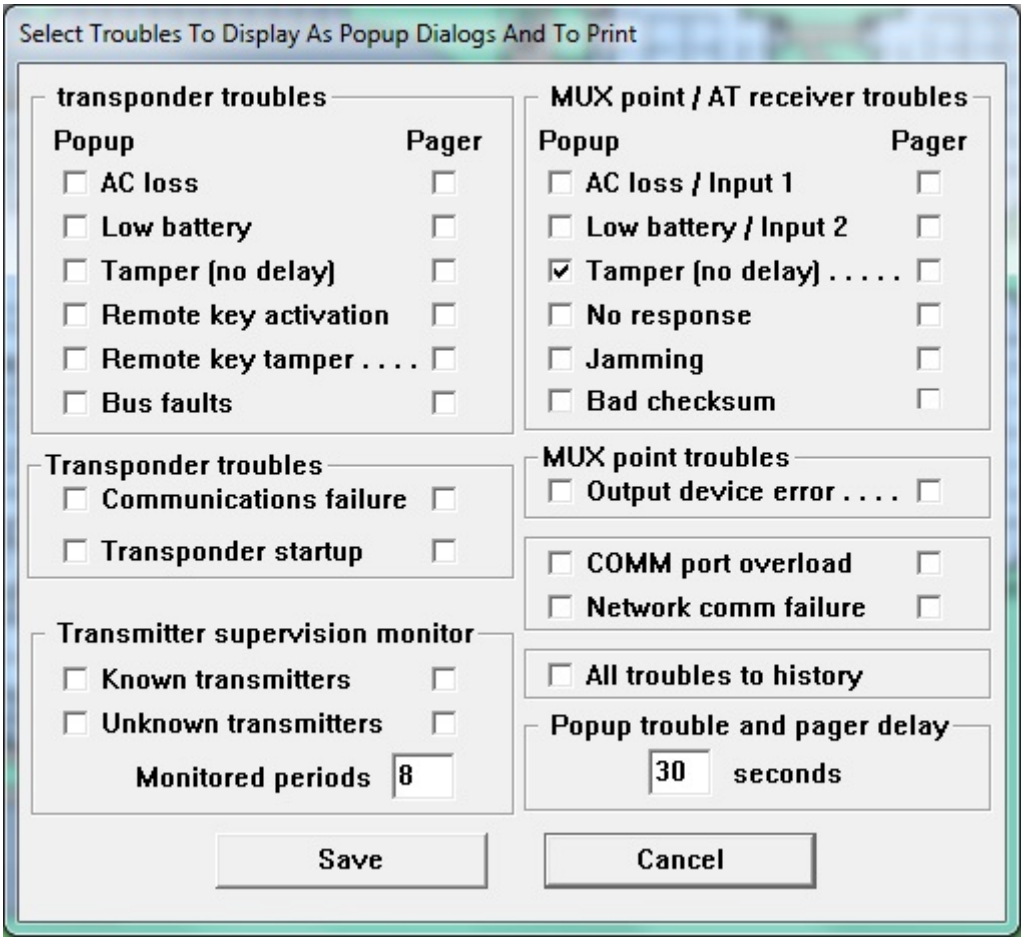


Figure 8.15: Popup Trouble Filter Dialog

Transponder troubles group

Communications failure To continually assure that communications between the Central Console and each transponder are functioning properly, each transponder is required to send a message to the Central Console periodically. If there is no response from the transponder, the Central Console displays a communications failure warning and records the condition in the audit file.
If a transponder determines it lost communications with the Central Console, it assumes control of the outputs of the devices connected to it and transmits “I’M OK” messages until it is acknowledged by the Central Console.

Notice!

If during this loss of communications, an alarm transmission is received by one or more of the receivers attached to the transponder, the transponder activates any alert units attached to it as well as the horns and red LED’s on any of its receivers which detected the alarm transmission. Since the transponder does not have access to the **Subscriber Database**, it must assume that all transmitters are valid, so even unauthorized (not in the **Subscriber Database**) transmitters produce audible alarm indications (if the system is set for audible alarms in the **Set Security Preferences** dialog).

	The Central Console also attempts to reestablish communications by continually requesting transmissions from the transponder and listening on the communications channel. When communications are restored with the Central Console, the transponder transmits any alarm and trouble conditions that occurred during the communications loss. Control of the horns, LEDs, strobes, and sirens reverts to the Central Console. This approach to managing a communications loss assures that alarm events cannot go undetected even if the Central Console is out of operation temporarily.
AC loss	The transponder senses when it loses AC power and reports the condition to the Central Console. After a few seconds delay, the Central Console displays a pop-up alert and records the condition in the audit file. See **Transponder Current Status** dialog.
Low battery	Periodically during normal operation, the transponder tests its battery. If the test fails, it immediately reports the condition to the Central Console. After a few seconds delay, the Central Console displays a pop-up alert and the condition is recorded in the audit file.
Tamper	The transponder immediately senses and reports the actuation of its tamper switch. The Central Console immediately displays a pop-up alert and records the condition in the audit file. Tamper reports are not delayed by the pop-up trouble and pager delay.
Remote key activation	The transponder immediately senses and reports the activation (shorting) of its remote key input when it is enabled in the **Transponder Parameter** dialog. The Central Console displays a pop-up alert and records the condition in the audit file.
Remote key tamper	The transponder immediately senses and reports the fault (open) of its remote key input when it is enabled in the **Transponder Parameter** dialog. The Central Console immediately displays a pop-up alert and records the condition in the audit file.
Transponder startup	The transponder reports to the Central Console when it first starts up. This can be caused by a technician turning the transponder on or by a watchdog failure of the on board microprocessor. The Central Console immediately displays a pop-up alert and records the condition in the audit file.
Bus faults	When the transponder is unable to communicate to any receivers or alert units on one or more of its multiplex busses, it immediately reports the condition to the Central Console. The Central Console reports the condition by means of a pop-up alert if the condition persists more than a few seconds. The condition is also recorded in the audit file.

MUX bus point troubles group

AC loss	The microprocessor of the alert unit detected the absence of AC power. Loss of AC power affects only the strobe and siren functions of the alert unit. Batteries provide backup power for the strobes and sirens. The logic and communications functions derive their power from the multiplex bus.
Low Battery	The alert unit tested for a low battery condition and the test failed.
Tamper	Whenever the cover is removed from a receiver or alert unit, the on-board microprocessor detects the tamper and it is reported to the transponder. Tamper reports are not delayed by the pop-up trouble and pager delay.
No response	Whenever a receiver fails to respond to a command from the transponder, a “No Response” message is sent by the transponder to the Central Console. This can occur if a multiplex bus wire is cut or a device is damaged.
Jamming	Each receiver monitors the level of radio energy being received at all times. If the level exceeds a preset threshold, for a preset length of time, the on-board microprocessor reports jamming.
Output device error	The transponder generates this message when it commands a receiver or alert unit to activate or deactivate an output device (siren, strobe, horn, or LED) and the device fails to respond correctly.
Bad checksum	This message is generated by the transponder and sent to the Central Console whenever the transponder detects message errors in the communications between receivers and alert units.

Transmitter supervision monitoring group

Known transmitters	To continually monitor the status of all transmitters programmed in the database that send periodic supervision transmissions. If any monitored transmitters stop sending supervision transmissions, a pop-up trouble is displayed.
Unknown transmitters	To monitor for periodic supervision transmissions from transmitters not programmed in the database, a pop-up trouble displays if transmissions from transmitters not programmed in the database are received.
Monitored periods	This is the number of supervision intervals that are consecutively missed before a pop-up screen reports a specific transmitter stopped reporting supervision transmissions.

Communications port monitor

Comm port overload	A pop-up trouble screen displays if the communications traffic to the transponders exceeds the system is capability.
Network comm failure	A pop-up trouble screen displays if the communications between the master and slave computers fails.

Delay to ignore troubles that auto reset

Pop-up trouble and pager delay The delay in seconds before a trouble displays on the computer screen. If a restore for a trouble is received before a trouble is displayed (this delay expires), the trouble and the restore are ignored. Tamper troubles are not delayed.

8.3.4 Transponder Parameter Change

This dialog allows parameters stored in the transponder's EEPROM memory to be viewed and changed.

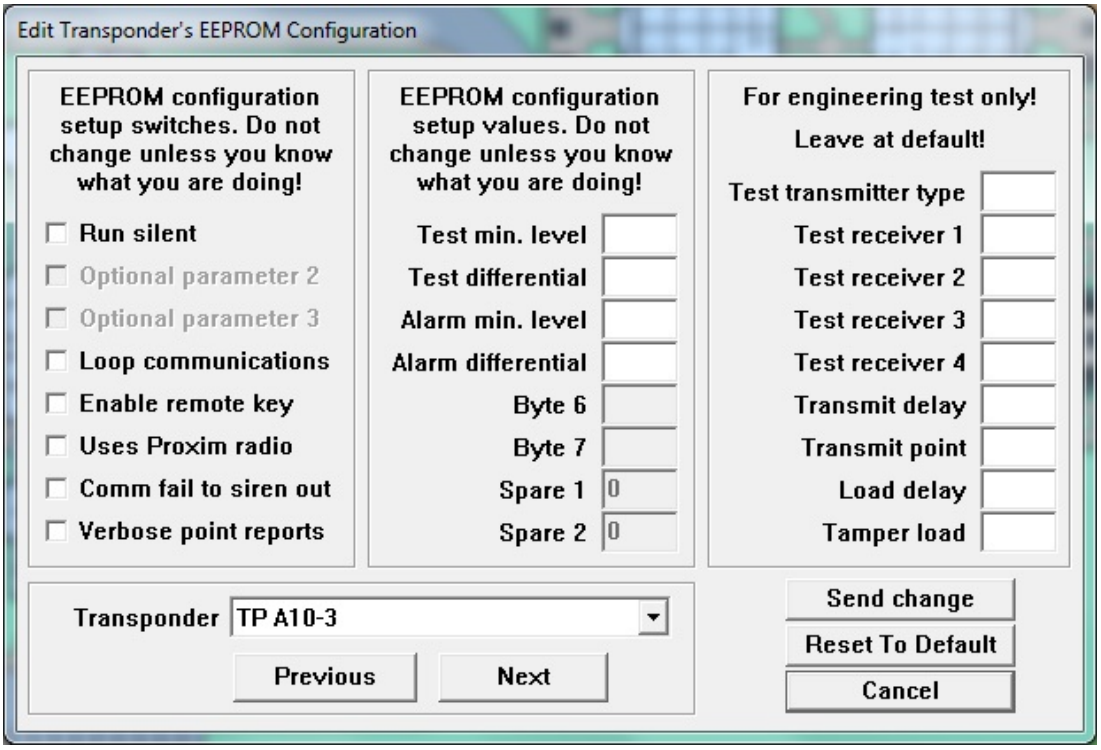


Figure 8.16: Transponder Parameter Change Dialog

Run silent If checked, the receivers and alert units on this transponder do not sound an alarm. This includes alarms received during a communications failure with the Central Console.

Optional parameter This option is currently disabled and reserved for future use.

Loop communications Normally the transponders are connected in parallel (party line) so they can all hear if any other transponders are in communications so they don't collide when communicating. However if fiber optic communications is used between the transponders and PC they can't be connected this way. Therefore they are connected in a loop. The transmission from the PC goes to the receiver on the first transponder. The transmission from the first transponder goes to the receiver on the second transponder and so on, until the transmission from the last transponder goes to the receiver on the PC. This option tells the transponders they are connected this way so it can react. You must make this change to the first transponder first, followed with the second, continuing in order until all is done.

Enable remote key(	If checked, the remote key supervised input on this transponder is enabled. Otherwise it will be ignored.
Uses Proxim radio	Only check this item if a Proxim radio is used to communicate to the Central Console.
Comm fail to siren out	If this item is checked, the siren output on this transponder activates when a communications failure is detected at the Central Console.
Verbose point reports	If checked, alarm and test reports include average levels and packet count information. This extra information is for diagnostic proposes only and is not required for system operation. Since the additional data increases the system traffic load leave this item unchecked.
Test min level	This is the minimum receive level (1 to 255) a receiver must see before the green light displays acknowledging a successful test. Leave this item at default (128).
Test differential	This is the minimum difference in receive level (1 to 255) a receiver must be less than the loudest receiver hearing a test before the green light displays acknowledging a successful test. Leave this item at default (64).
Alarm min level	This is the minimum receive level (1 to 255) a receiver must see before the sounder and red light is displayed for an alarm. Leave this item at default (1).
Alarm differential	This is the minimum difference in receive level (1 to 255) a receiver must be less than the loudest receiver hearing an alarm before the sounder and red light are displayed for an alarm. Leave this item at default (255).
Byte	These are future options, leave at default (0).
Spare	These are future options, leave unchecked..
Test transmitter type **Test receiver 1, 2, 3, 4** **Transmit delay** **Transmit point** **Load delay** **Tamper load**	These parameters are used for engineering system load testing only. **Do not use in a live system**, as they can generate more traffic than a system can handle; therefore, actual alarms may be missed. Leave them at default.
Transponder	Selects the transponder the data is presented for.
[Previous]	Returns to the previous transponder in the system.
[Next]	Advances to the next transponder in the system.
[Send change]	Sends the changes made to the selected transponder. Changes are not made to the transponder EEPROM memory unless this button is clicked.
[Reset to Default]	Reset the selected transponder to the default settings.
[Cancel]	Cancel the operation and close the dialog window.

8.3.5 Transponder Data View

This dialog is solely for engineering evaluation of the transponder only.

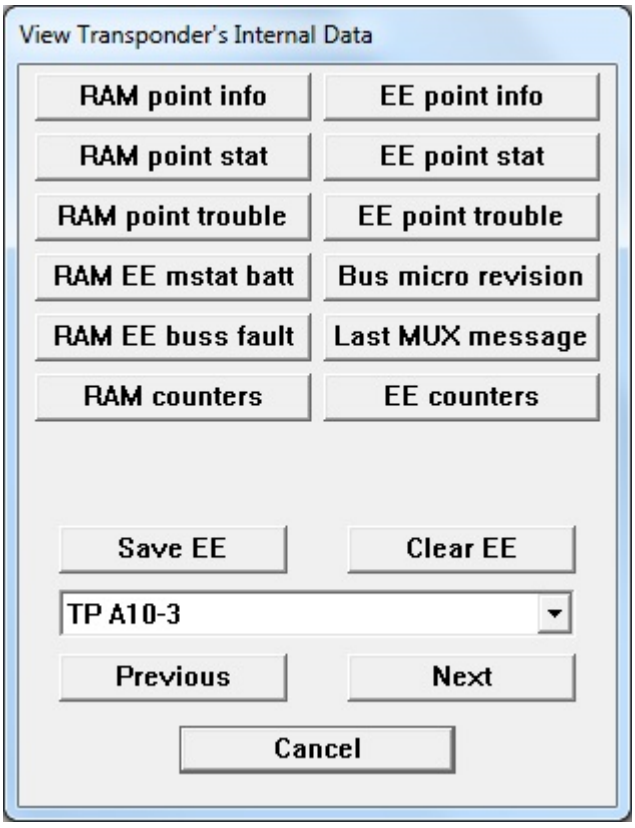


Figure 8.17: Transponder Data View Dialog

[RAM point info]	Views the RAM image of point information.
[RAM point stat]	Views the RAM image of point status.
[RAM point trouble]	Views the RAM image of point trouble.
[RAM EE mstat batt]	Views the RAM and EEPROM images of transponder status and battery condition.
[RAM EE buss fault]	Views the RAM and EEPROM images of transponder MUX bus fault condition.
[RAM counters]	Views the RAM image of the process registers.
[EE point info]	Views the EEPROM image of point information.
[EE point stat]	Views the EEPROM image of point status.
[EE point trouble]	Views the EEPROM image of point trouble.
[Bus micro revision]	Views the bus micro revision for the connected points.
[Last MUX message]	Views the last MUX bus message received.
[EE counters]	Views the EEPROM image of the process registers.
[Save EE]	Saves the current RAM image to the EEPROM memory on the transponder.
[Clear EE]	Clears the EEPROM memory on the transponder and resets the transponder.
[Previous]	Returns to the previous transponder in the system.

[Next]	Advances to the next transponder in the system.
[Cancel]	Cancels the operation and closes the dialog window.

8.3.6 Receiver configuration dialog

Once the receiver and alert unit data for a transponder has been entered into the **Transponder Database**, this dialog is used to verify that each receiver is working and is properly addressed in the database. This setup tool identifies errors in the address switch settings of receivers and alert units as well as data entry errors in the **Transponder Database**.

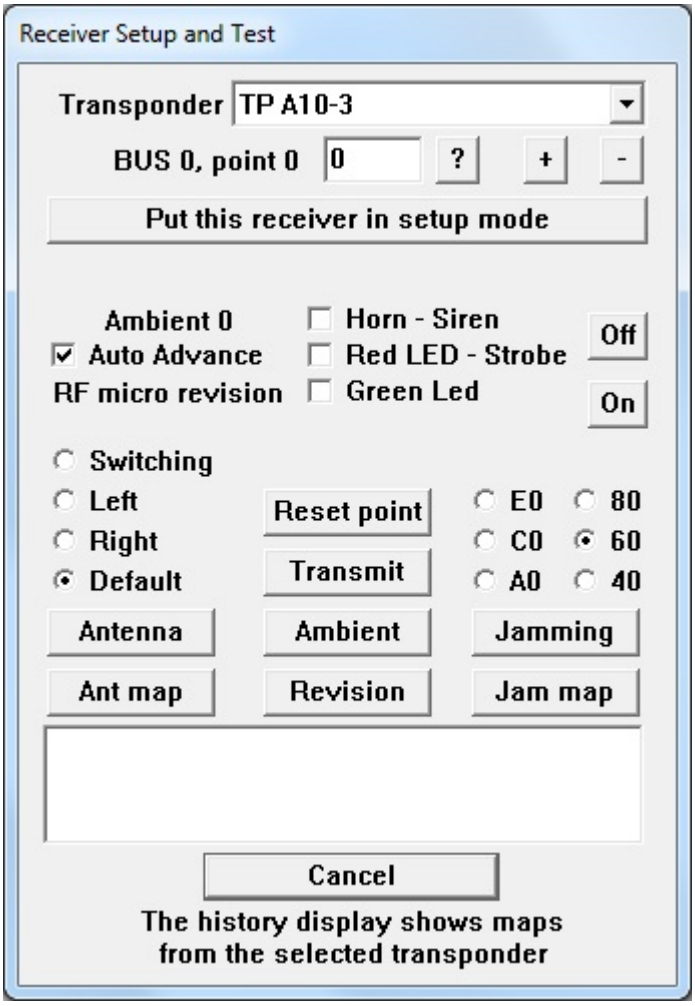


Figure 8.18: Receiver Configuration Dialog

[Put this receiver in setup mode]	This button initiates the setup process by causing both the red and green LED of the selected receiver to light up. The red and green LED will be flashing. On the Central Console, this button changes the **[Abort setup for this MUX Point]** button to be able to proceed to the next device in the event that one receiver is not set up properly.
Ambient value	The **Ambient** value, shown above **Auto Advance,** shows the current ambient level at the receiver. To get an updated ambient reading, select the point and click the **[Transmit]** button followed by the **[Ambient]** button.
Auto Advance	If this checkbox is checked, the Central Console automatically selects the receiver with the next higher point address.
RF micro revision	The receiver's RF micro revision level is shown below **Auto Advance**. To get an updated reading, click the **[Revision]** button.
Horn - Siren	If this checkbox is checked, the horn output of a receiver or the siren output of an alert unit is turned on upon clicking the **[On]** button, or turned off upon clicking the **[Off]** button. If this checkbox is not checked, the state of this output does not change.
Red LED - Strobe	If this checkbox is checked, the red LED output of a receiver or the strobe output of an alert unit is turned on upon clicking the **[On]** button, or turned off upon clicking the **[Off]** button. If this checkbox is not checked, the state of this output does not change.
Green Led	If this checkbox is checked, the green LED output of a receiver or the spare output of an alert unit is turned on upon clicking the **[On]** button, or turned off upon clicking the **[Off]** button. If this checkbox is not checked, the state of this output does not change.
[Off]	Upon clicking the button, any checked outputs (**Horn-Siren**, **Green LED**, **Red LED - Strobe**) is turned off for the selected point on the selected transponder. If the output does not change, click the **[On]** button followed by the **[Off]** button again.
[On]	Upon clicking the button, any checked outputs (**Horn-Siren**, **Green LED**, **Red LED - Strobe**) is turned on for the selected point on the selected transponder. If the output does not change, click the **[Off]** button followed by the **[On]** button again.
[Antenna]	Normally, a receiver automatically switches between its diversity antennas during normal operation (leave the default selection on a working system at this setting). The receiver can be forced to use only the left or right antenna, or always switch by selecting the appropriate setting and clicking the **[Antenna]** button.

[Ant map]	Clicking the **[Ant map]** button causes the system to interrogate the current antenna switching settings of all receivers on this transponder.
[Reset point]	Clicking the **[Reset point]** causes the microprocessors on this point to reset as if they were just powered up. A receiver should not be reset in a working system, as it can cause receptions to be lost.
[Transmit]	Clicking the **[Transmit]** button causes this receiver to send one test transmission.
[Ambient]	Clicking the **[Ambient]** button causes the system to interrogate the current ambient levels of all receivers on this transponder.
[Revision]	Clicking the **[Revision]** button causes the system to interrogate the RF micro revision levels of all receivers on this transponder.
[Jamming]	A receiver monitors the ambient level during normal operation. If the ambient level rises above the jamming setting and jamming trouble, it is reported to the Central Console. The receiver's jamming level can be adjusted by selecting the appropriate setting (shown in hexadecimal levels) and clicking the **[Jamming]** button.
[Jam map]	Clicking the **[Jam map]** button causes the system to interrogate the jamming setting levels of all receivers on this transponder.
[Cancel]	Clicking the **[Cancel]** button closes the dialog window.

Put this receiver in setup mode
This button initiates the setup process by causing both the red and green LED of the selected receiver to light up. The red and green LED will be flashing. On the Central Console, this button changes the **[Abort setup for this MUX point]** button to be able to proceed to the next device in the event that one receiver is not set up properly.
The next step is using a maintenance transmitter to transmit an alarm while standing near the receiver.

Notice!
The illuminated LED indicate to the service person standing near the device that the receiver is actually the one currently in the setup mode. If the LED of the designated receiver are not illuminated, there is probably an error in the switch settings of the receiver or an error in the address in the **Transponder Database**. To help resolve such problems, the person at the Central Console can command any device to illuminate its LED and/or sound its horn.

If the receiver in the setup mode detects the maintenance alarm and if the received signal is the strongest of all receivers, the horn on the receiver sounds briefly and the LEDs go off. This indicates the receiver is functioning properly and the receiver's address is set correctly in the **Transponder Database** and on the receiver's switches.

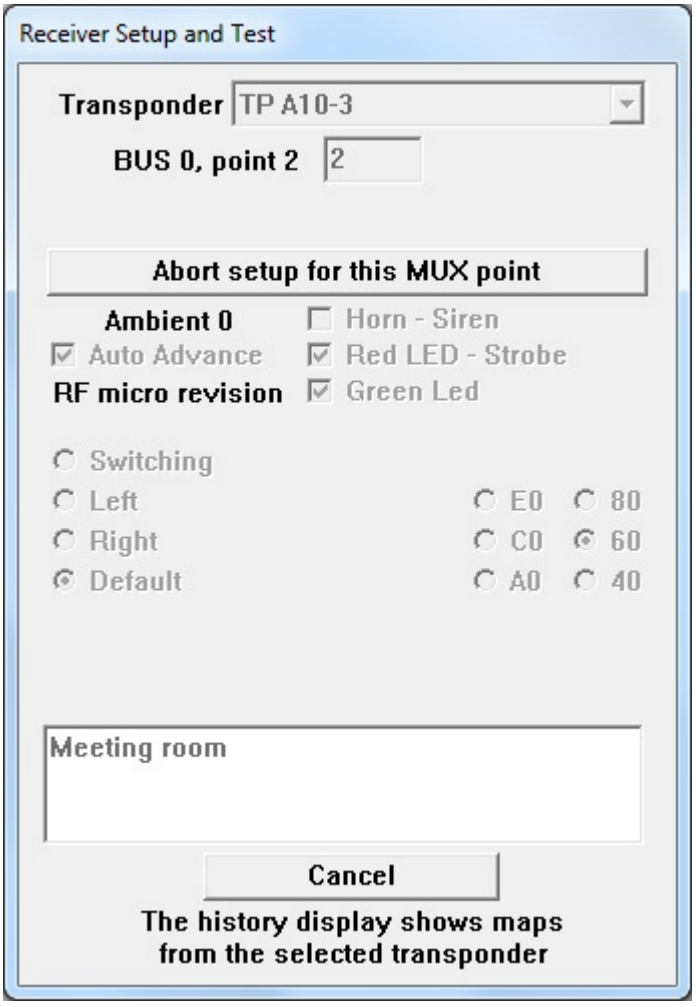


Figure 8.19: Abort Button to Remove a Device from the Setup Mode

The Central Console also confirms the successful setup with an audible and text message. The **[Abort setup for this MUX point]** button disappears and is replaced by **[Test on this MUX point SUCCESSFUL]** button. Click this button to conclude the test on this point.

8.3.7 Receiver test dialog

Use this dialog to set up and monitor four receivers, and listen to one receiver transmitting with its buddy check transmitter. Normally, the function is for engineering evaluation of new transmitter and receiver designs, but it can be used to test receiver boards and locations in a working system.

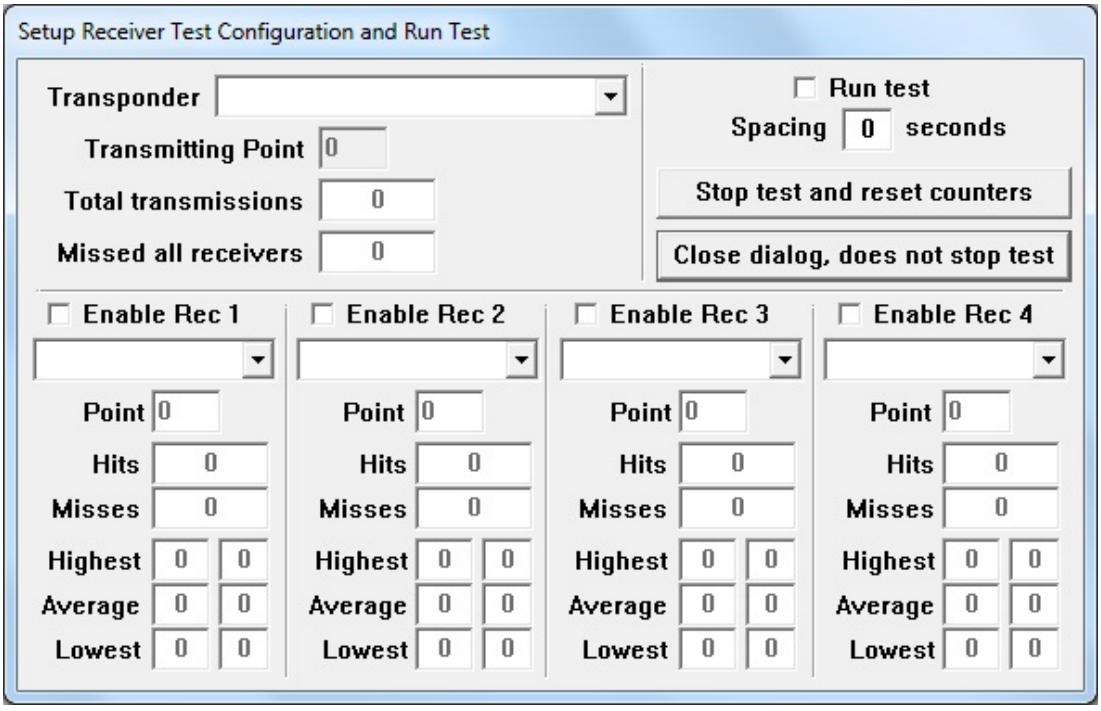


Figure 8.20: Receiver Test Dialog

Transponder	Select the transponder for the transmitting point and each receiving point. They can be on the same or different transponders.
Transmitting Point	Select the point (receiver) on the selected transponder to generate the transmissions.
Total transmissions	The total number of times the designated receiver transmitted the test message.
Missed all receivers	The total number of times where the test transmission was not heard by any of the designated receivers.
Enable Rec	This checkbox must be checked for this receiver to monitor the test transmissions.
Point	Select the point (receiver) on this transponder to monitor the test transmissions.
Hits	The number of times this receiver successfully heard the test transmission.
Misses	The number of times this receiver failed to hear the test transmission.
Highest	The left box displays the highest receive level at which the test transmission was heard. The right box displays the greatest number of packets heard from a single test transmission.
Average	The left box displays the average receive level at which the test transmission was heard. The right box displays the average number of packets heard from a single test transmission.

Lowest	The left box displays the lowest receive level at which the test transmission was heard. The right box displays the least number of packets heard from a single test transmission.
Run test	The test only runs when this checkbox is checked. To stop the test and retain the test values, uncheck this checkbox.
Spacing	This slows the test by forcing this number of seconds between test transmissions. Normally, this setting is left at the default of 0.
Stop test and reset counters	Clicking this button stops the test and resets all values.
Close dialog, does not stop test	Clicking this button closes this dialog but does not stop the test from running. Reopening the dialog displays the current progress of the test. The test should not be left running unless there is a specific need, as it generates both RF and system traffic.

8.3.8 Network status dialog

This dialog shows the status of communications on the network, modem, and system serial ports.

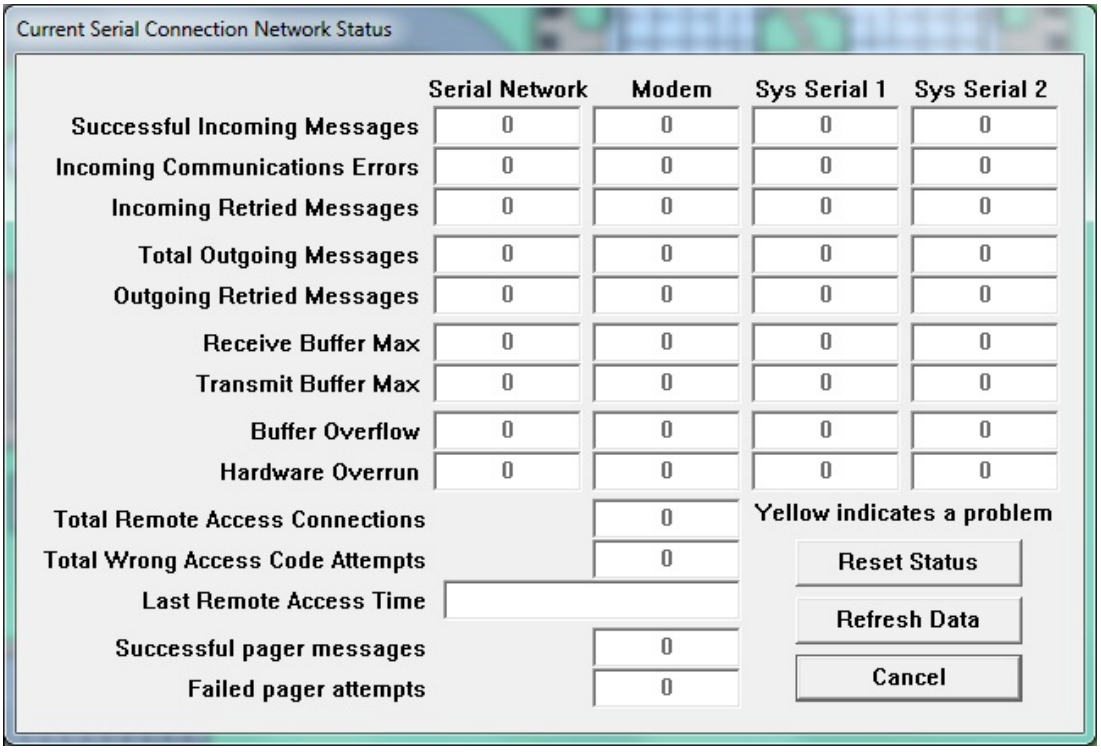


Figure 8.21: Network Status Dialog

Successful Incoming Messages	This value is the number of messages that the system successfully received on this communication port.
Incoming Communication Errors	This value is the number of messages that the system detected errors in, on this communication port. If displayed in yellow, this value is more than 1.5% of the **Successful Incoming Messages**.
Incoming Retried Messages	This value is number of successful receptions that indicated that they retried by the sending application. If displayed in yellow, this value is more than 1.5% of the **Successful Incoming Messages**.
Total Outgoing Messages	This value is total number of outgoing messages sent on this port.
Outgoing Retried Messages	This value is number of outgoing messages that were retried because the receiving application did not acknowledge them. If displayed in yellow, this value is more than 1.5% of the **Total Outgoing Messages**.
Receiver Buffer Max	This value is maximum number of bytes received on this serial port, but not yet processed by the system. If displayed in yellow, more than 50% of the queue was in use.
Transmit Buffer Max	This value is maximum number of bytes processed by the system, but not yet transmitted on this serial port. If displayed in yellow, more than 50% of the queue was in use.
Buffer Overflow	This is the number of times a byte was lost by the software for a serial port because the input buffer overflowed. Bytes were placed into the input buffer faster than the system could process them.
Hardware Overrun	This is the number of times a byte was lost by the hardware for a serial port because it was not fast enough to process the byte into the input buffer.
Total Remote Access Connections	This value is the total number of times a remote access connection was successful.
Total Wrong Access Code Attempts	This value is the number of times a remote access connection was attempted and rejected because a valid remote access code was not received.
Last Remote Access Time	This is the time and date of the last successful remote access attempt.
Successful pager messages	This value is the number of successful pager messages sent.
Failed pager attempts	This value is the number of times a pager message dial-out was unsuccessful.
[Reset Status]	Clicking this button resets all values shown in this dialog.
[Refresh Data]	Clicking this button refreshes all values shown in this dialog. The values are not automatically updated when the dialog is left open.
[Cancel]	Clicking this button closes the dialog window.

8.3.9 System status dialog

This dialog shows the status of internal system queues and communications on the serial ports assigned to transponders.

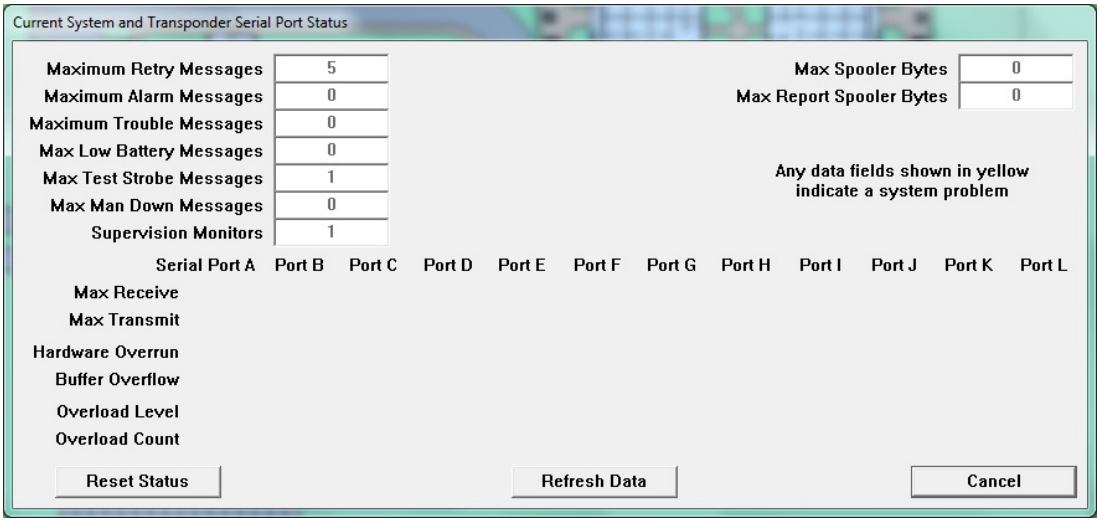


Figure 8.22: System Status Dialog

Maximum Retry Messages This value is maximum number of messages in queue to be sent to all transponders in the system, and were not yet acknowledged. If displayed in yellow, more than 50% of the queue was in use at this value.

Maximum Alarm Messages This value is the maximum number of alarms that the system processed at its busiest time. If displayed in yellow, more than 50% of the maximum was in use.

Maximum Trouble Messages This value is the maximum number of troubles in the queue yet to be displayed. If displayed in yellow, more than 50% of the queue was in use.

Max Low Battery Messages This value is the maximum number of transmitters with low batteries yet to be displayed. If displayed in yellow, more than 50% of the queue was in use.

Max Test Strobe Messages This value is the maximum number of test strobes in use at one time. If displayed in yellow, more than 50% of the queue was in use.

Max Man Down Messages This value is the maximum number of transmitters timing man down events, at one time. If displayed in yellow, more than 50% of the queue was in use.

Supervision Monitors This value is the current number of transmitters being monitored for supervision transmissions.

Max Spooler Bytes This value is the maximum number of bytes spooled for the printer at one time. If displayed in yellow, more than 50% of the queue was in use.

Max Report Spooler Bytes	This value is the maximum number of bytes spooled for the printer for Guard Tour Reports at one time. If displayed in yellow, more than 50% of the queue was in use.
Max Receiver Buffer	This value is the maximum number of bytes received from transponders on this serial port, but not yet processed by the system. If displayed in yellow, more than 50% of the queue was in use.
Max Transmit Buffer	This value is the maximum number of bytes processed by the system, but not yet transmitted to the transponders on this serial port. If displayed in yellow, more than 50% of the queue was in use.
Hardware Overrun	This is the number of times a byte was lost by the hardware for a serial port because it was not fast enough to process the byte into the input buffer.
Buffer Overflow Count	This is the number of times a byte was lost by the software for a serial port because the input buffer overflowed. Bytes were placed into the input buffer faster than the system could process them.
Overload Level	This is a measure of the amount of time peak traffic on this serial port was greater than the system's ability to handle it. The system automatically sheds non-essential tasks when this value rises.
Overload Count	This is a measure of the number of times peak traffic on this serial port was greater than the system's ability to handle it. The system automatically sheds non-essential tasks when this value rises.
[Reset Status]	Clicking this button resets all values in this shown in this dialog.
[Refresh Data]	Clicking this button refreshes all values shown in this dialog. The values are not automatically updated when the dialog is left open.
[Cancel]	Clicking this button closes the dialog window.

8.3.10 Pager setup dialog

This dialog sets up remote pager access for troubles (service) and alarms (security).

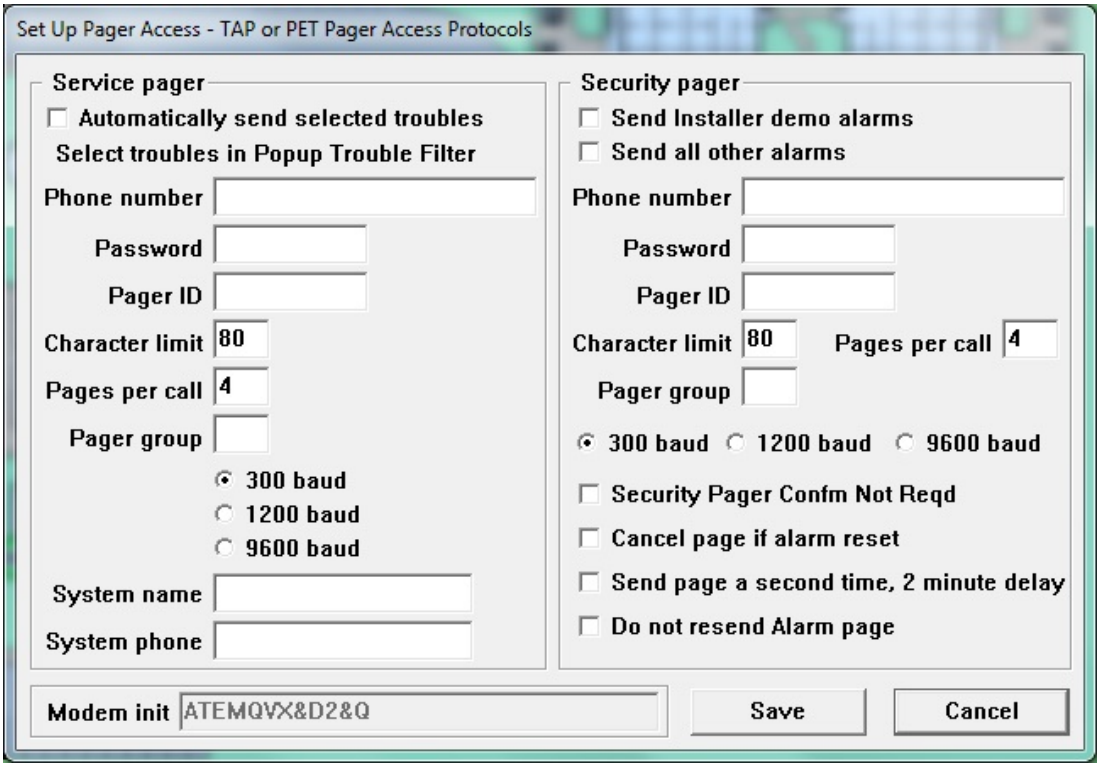


Figure 8.23: Pager Setup Dialog

Automatically send selected troubles	If checked, send the troubles selected in the **Popup trouble filter** dialog to the service pager.
Phone number	Phone number to be dialed to access the paging service. This phone number is usually different from the number you would manually dial to send a page. The paging company assigns this value.
Password	This is the password that must be sent to the paging service to send the page. If not required, leave this field black. Usually a password is not required. The paging company assigns this value.
Pager ID	This is the ID that identifies the specific pager that this message is to be sent to. Many times, it is the last 7 digits of the phone number that you would manually dial to access this pager. The paging company assigns this value.
Character limit	This is the maximum number of characters allowed per page. Typically, this is set to 80 characters. The Security Escort System will truncate the pager message at this number of characters. The paging company assigns this value.
Pages per call	This is the maximum number of pager messages allowed per phone call. Typically, this is set to 4 pages per call. When this number of messages have been sent, and there are more messages to be delivered; the Security Escort System will hang up and redial the paging service to deliver the remaining messages. The paging company assigns this value.

Pager group	This is the group of up to 8 pagers that this message is to be sent to. You may program the individual pager as well as a group of pagers. The pager group will be sent the page before the individual.
Baud rate	This is the baud rate that will be used to communicate with the paging computers. The paging company assigns this value.
System name	This identifies the Security Escort System when multiple Security Escort Systems report to the same service pager. Keep this field as short as reasonably possible since these characters, including space character, will be sent before each trouble message and they are included in the **Character limit** set above. If not desired, leave blank.
System phone	This will present phone number to be called in response to the service page. Only use if required since these characters, plus a space, will be sent before each trouble message. They are included with the **System name** in the **Character limit** set above. If not desired, leave blank.
Send installer demo alarms	If checked, demo alarms will be sent to the security pager.
Send all other alarms	If checked, all actual alarms will be sent to the security pager.
Security Pager Confm Not Reqd	If checked, the confirmation pager message is not sent to the security pager when the alarm is acknowledged by an acknowledgement transmitter.
Cancel page If alarm reset	If checked, the alarm page will be canceled if the alarm is reset before it can be communicated to the paging service.
Send page a second time, 2 minute delay	If checked an alarm page will be sent a second time to the security pager. Do this in case the pager was in an area where pages could not be heard when the first page was sent.
Do not resend alarm page	If checked, a pager message is sent to the security person only once till the alarm is cancelled or acknowledged.
Modem init	This is the initialization string sent to the modem to set it up for pager communications. Normally, this setting would not have to be changed. To allow changes to this string, hold down the <Shift> + <Ctrl> keys when this dialog is first opened. This string is specific to each modem model. The default setting should work with most modems.
[Save]	Save the changes and close the dialog window.
[Cancel]	Cancel the changes and close the dialog window.

8.3.11 Send pager message dialog

Allows manually entered messages to be sent to the service or security pagers. Service and security pagers are configured in the **Pager setup** dialog. Individuals and group pager assignments are configured in the **Subscriber Database**.

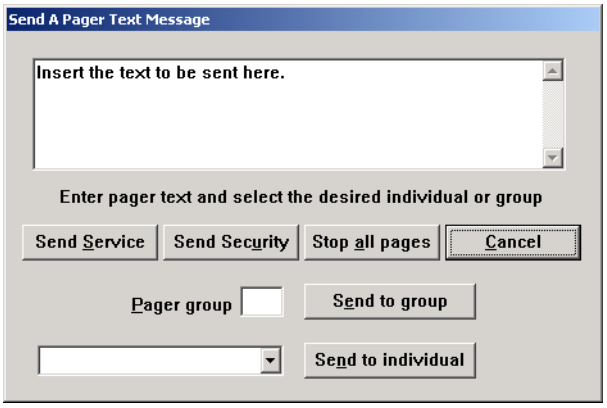


Figure 8.24: Send Pager Message Dialog

Insert the text to be sent here.	Enter the text to be sent to the pagers in the large text box at the top of the dialog.
[Send Service]	Causes the entered message to be sent to the service pager and service pager group.
[Send Security]	Causes the entered message to be sent to the security pager and security pager group.
[Stop all pages]	Causes all pages currently queued (automatic or manual) to be aborted and deleted. Use with caution.
Pager group	To send a page to all members of a group, enter the pager group number here (1 to 99).
[Send to group]	Click this button to send the text entered to the indicated pager group.
[Send to Individual]	Click this button to send the text entered to the individual that is selected from the drop down list.
[Cancel]	Cancel and close this dialog window..

8.4 Print history screen

This selection will print the current data in the **History Screen** buffer to the report printer.

8.4.1 Print file dialog

Enter the name of the file to be printed or click the **[Browse...]** button to open the **Common Open File** dialog. Then click the **[Print]** button to print the file to the report printer.

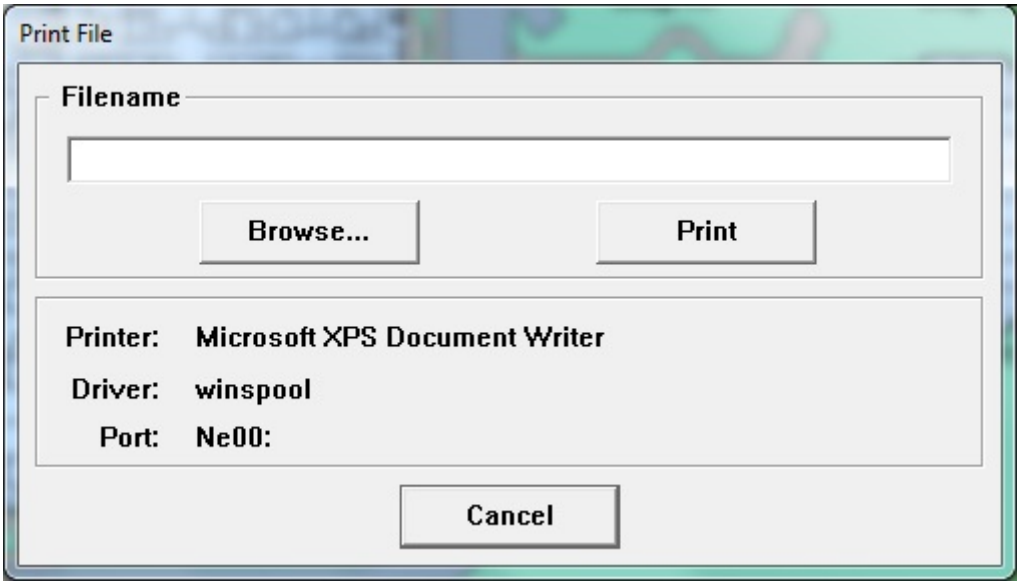


Figure 8.25: Print File Dialog

This is the standard Windows **Common Open File** dialog that is used for selecting the file to be printed. It works the same as any other Window's standard application.

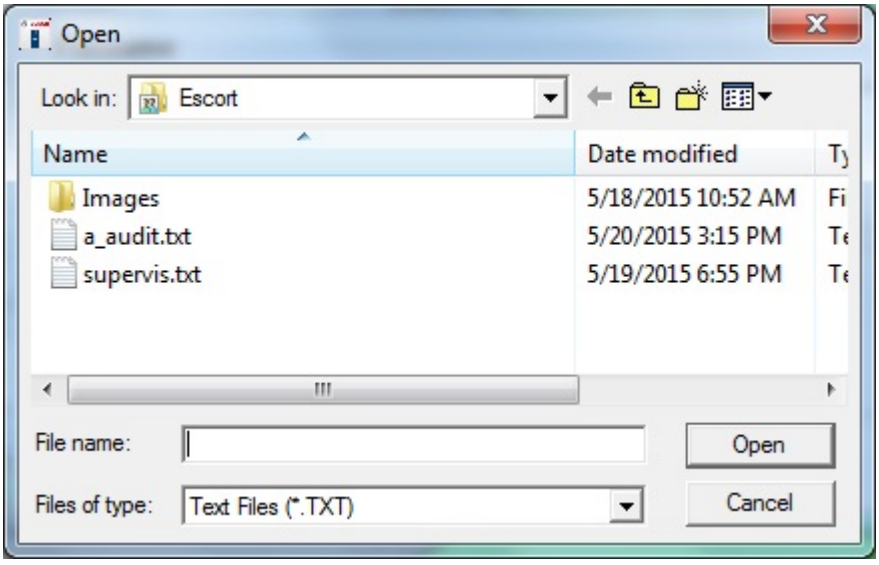


Figure 8.26: Common Open File Dialog

8.5 Network menu

This is the network menu used to set up and monitor the TCP/IP network and the computer's file paths.

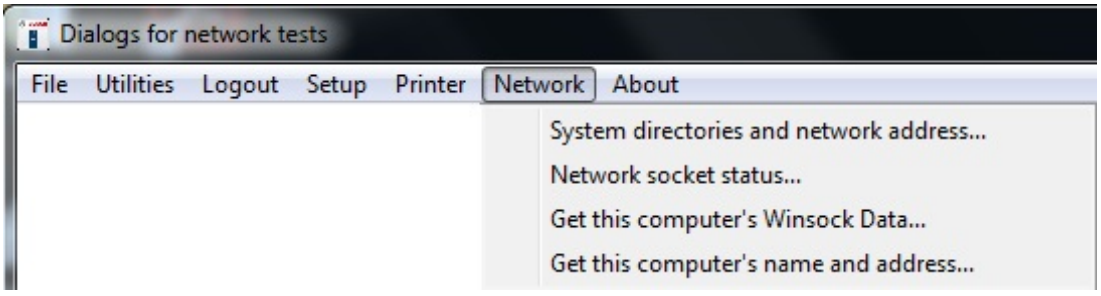


Figure 8.27: Network Menu

8.5.1 System Directories and Network Address Dialog

Use this dialog to set up the network IP addresses, ports and related options. File paths can also be configured.

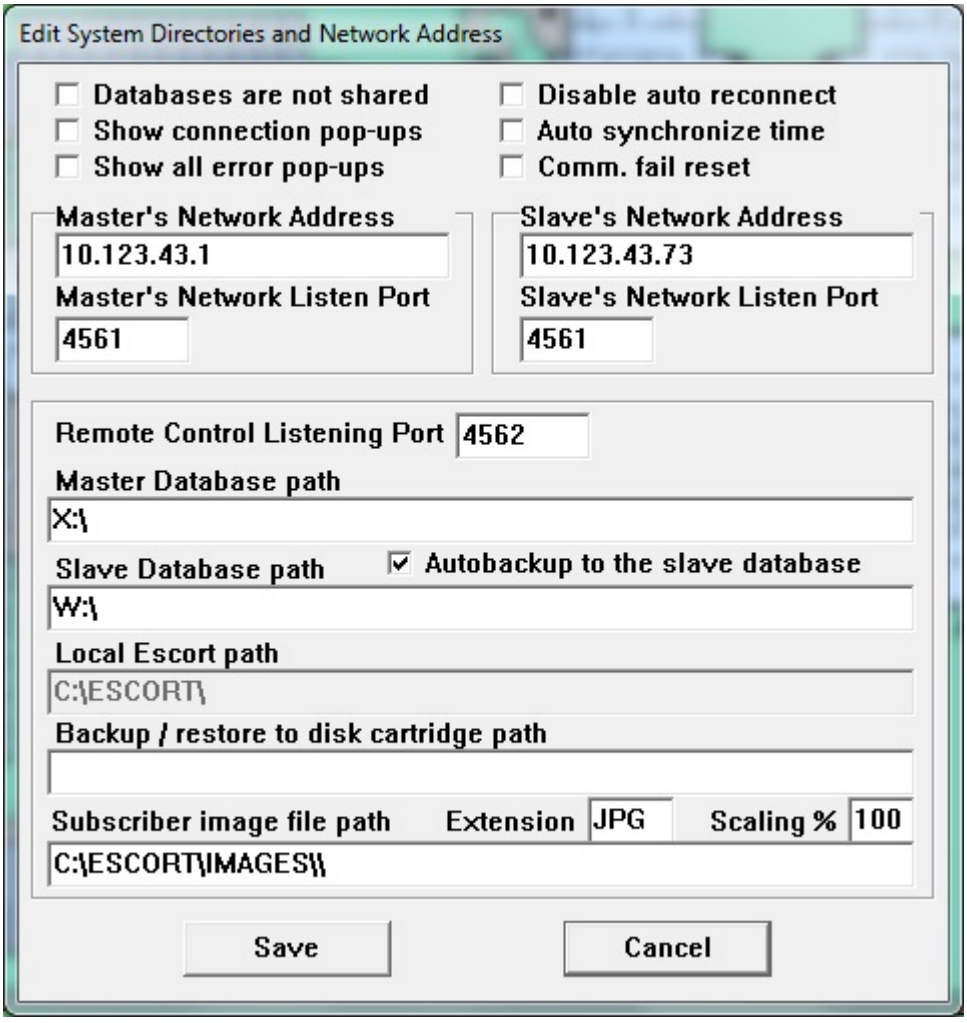


Figure 8.28: System Directories and Network Address Dialog

Databases are not shared	If this option is not checked, the master and all the slave and workstation computers share the same database files. This checkbox must only be checked if each computer has its own copy of the databases stored locally. In normal operation, this checkbox is typically unchecked. If this checkbox is checked, the databases must be manually updated using **Backup** and **Restore** every time changes are made to the database.
Show connection pop-ups	If this option is checked, it will display a pop-up message box whenever a network connection is initiated or released with another computer. Unchecking this checkbox stops the message boxes from displaying. In normal operation, this checkbox is typically unchecked.
Show all error pop-ups	If this option is checked, it will display a pop-up message box whenever a network error is reported. Unchecking this checkbox stops the message boxes from displaying. In normal operation, this checkbox is typically unchecked.
Disable auto reconnect	If this option is checked, the system will not automatically attempt to reconnect a lost connection each minute. Unchecking this checkbox allows the system to automatically reconnect a lost connection. In normal operation, this checkbox should be unchecked.
Auto synchronize time	If this option is checked, the master computer will automatically synchronize the time on the slave and workstation computers once each night.
Comm. fail reset	If this option is checked, the master computer will reset when communication failure occurs..
Master's Network Address:	The IP address of the master computer. The Security Escort system requires a fixed IP address for the master computer.
Master's Network Listen Port	A unique number that indicates the Security Escort software is attempting to set up a connection. Other software uses different port numbers, allowing the network interface card to be shared with other network applications. Typically, this is set as “4561”.
Slave's Network Address	The IP address of the slave computer. The Security Escort system requires a fixed IP address for the optional slave computer.
Slave's Network Listen Port	A unique number that indicates the Security Escort software is attempting to set up a connection. Other software uses different port numbers, allowing the network interface card to be shared with other network applications. Typically, this is set to “4561”.

[Learn address]	Clicking this button on the master computer automatically populates the master's IP address in the **Master's Network Address** textbox, and the master's network port in the **Master's Network Listen Port** textbox. Clicking this button on the slave computer automatically populates the master's IP address in the **Slave's Network Address** textbox, and the master's network port in the **Slave's Network Listen Port** textbox. If the computer has more than one network interface card (NIC), you must verify that the correct IP address was selected by comparing this address to the IP address that was programmed in the Control Panel TCP/IP protocol. If the address is not correct, manually enter the correct IP address.
Remote Control Listening Port	The Security Escort will be listening on this port to communicate with the OPC server. A separate OPC server is created to communicate between the OPC client and the Security Escort system. The OPC server holds the alarm and trouble messages, and sends the same to the available client once it is connected. The OPC server will send the status of the Security Escort to the OPC client. The OPC sever also acknowledges and deletes alarm and trouble messages from OPC client. If the connection between OPC server and Security Escort goes down, the OPC server will try to reconnect with Security Escort. Once the connection to the Security Escort becomes active, the Security Escort will send all the available alarms to the OPC server. The OPC server in turn sends the alarm back to OPC client; hence the OPC client may display some duplicate alarms.
Master Database path	The path that this slave or workstation computer uses to access the shared database files on the master computer. This path may have a different drive letter on the different slave and workstation computers. They are typically on the master computer, but they may be on a file server or any other network accessible drive. **Note: With version 2.04 and above of the software, it is possible to use UNC path names instead of mapping drive letters. Therefore, the path to the master computer's database would be "\\MASTER\ESCORT".**
Autobackup to the slave database	If this option is checked, the slave computer will back up all databases in the **Master Database path** to the **Slave Database path** each night at 3:00 am.

Slave Database path	The path that this master or workstation computer uses to access the hot backup database files on the slave computer. This path may have a different drive letter on the different master and workstation computers. They are usually on the slave computer, but they may be on a file server or any other network accessible drive. Typically, they would not be stored on the same computer as the **Master Database path**, so a single failure would not prevent access to both the master and slave database files. **Note: With version 2.04 or above of the software, it is possible to use UNC path names instead of mapping drive letters. Therefore, the path to the slave computer's database would be "\\SLAVE\ESCORT".**
Local Escort path	The path on this workstation where the Security Escort was installed in. Typically it is "C:\ESCORT".
Backup / restore to disk cartridge path	When backing up or restoring the databases to a disk cartridge, this is the path that is used.
Subscriber image file path	The Security Escort System software can display an image for each subscriber on the alarm screen. This parameter tells the software the path where the image files are stored. The default is "C:\ESCORT\IMAGES".
Extension	The subscriber images can be in JPEG or Windows Bitmap format. All images in a system must be in the same format. For the JPEG format, enter the Windows extension "JPG". For the Bitmap format, enter the Windows extension "BMP".
Scaling %	When the display is set to 640x480 pixels, and subscriber images are being displayed, this parameter controls the image size. This value can range from 10 to 100%, and should be adjusted while viewing alarms to get the desired image size. When the display is set to 800x600 or larger (recommended), this parameter has no effect.
[Save]	Clicking this button saves the changes and closes the dialog window.
[Cancel]	Clicking this button aborts the changes and closes the dialog window.

8.5.2 Network Socket Status Dialog

This dialog shows diagnostic information for the selected TCP/IP socket.

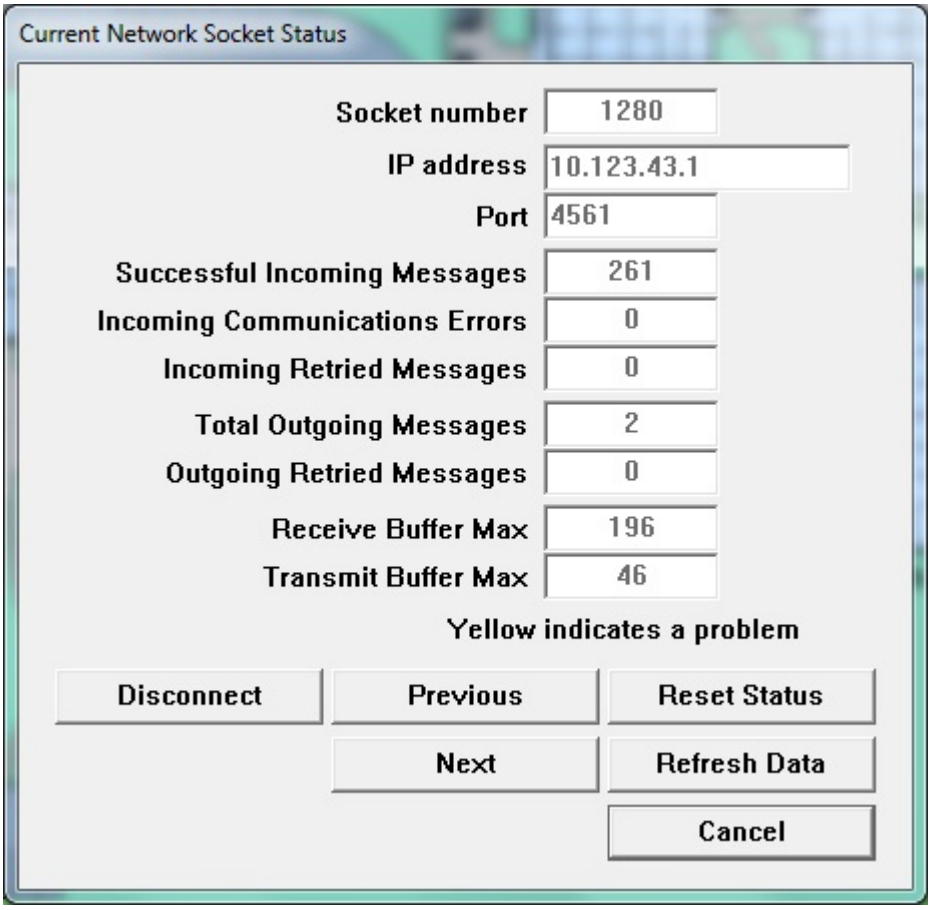


Figure 8.29: Current Network Socket Status Dialog

Successful Incoming Messages	Number of messages that the system has successfully received on this socket.
Incoming Communication Errors	Number of messages that the system detected errors in, on this socket. If displayed in yellow, this value is more than 1.5% of the **Successful Incoming Messages**.
Incoming Retried Messages	Number of successful receptions which indicated that the retries by the sending application. If displayed in yellow, this value is more than 1.5% of the **Successful Incoming Messages**.
Total Outgoing Messages	Total number of outgoing messages that were sent on this socket.
Outgoing Retried Messages	Number of outgoing messages that were retried because the receiving application did not acknowledge them. If displayed in yellow, this value is more than 1.5% of the **Total Outgoing Messages**.
Receive Buffer Max	Maximum number of bytes that were received on this serial port, but not yet processed by the system. If displayed in yellow, more than 50% of the queue was in use.
Transmit Buffer Max	Maximum number of bytes that were processed by the system, but not yet transmitted on this socket. If displayed in yellow, more than 50% of the queue was in use.

[Reset Status]	Clicking this button resets all values shown in this dialog.
[Refresh Data]	Clicking this button refreshes all values shown in this dialog. The values are not automatically updated when the dialog is left open.

8.5.3 Computer's Winsock Data Dialog

This dialog shows information about the Windows Winsock support. This is only used for diagnostic purposes.

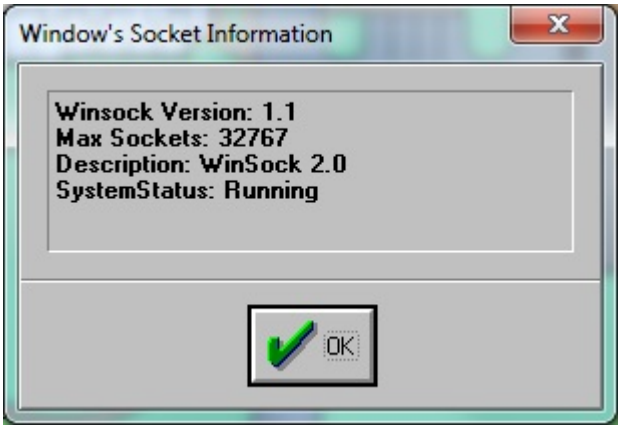


Figure 8.30: Computer's Winsock Data Dialog

8.5.4 Computer's Name and Address Dialog

This dialog shows the computer's network name and current IP address.

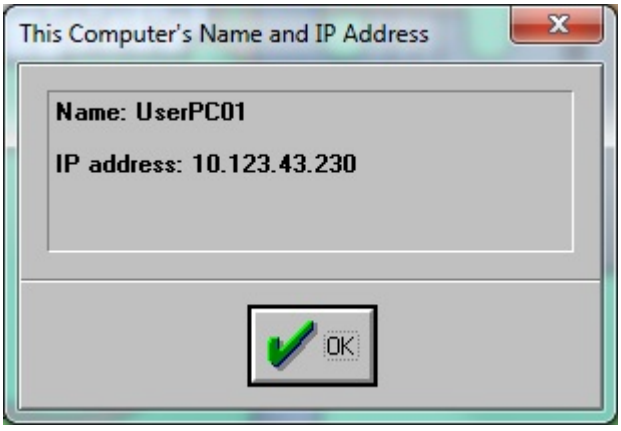


Figure 8.31: Computer's Name and IP Address Dialog

8.6 About menu

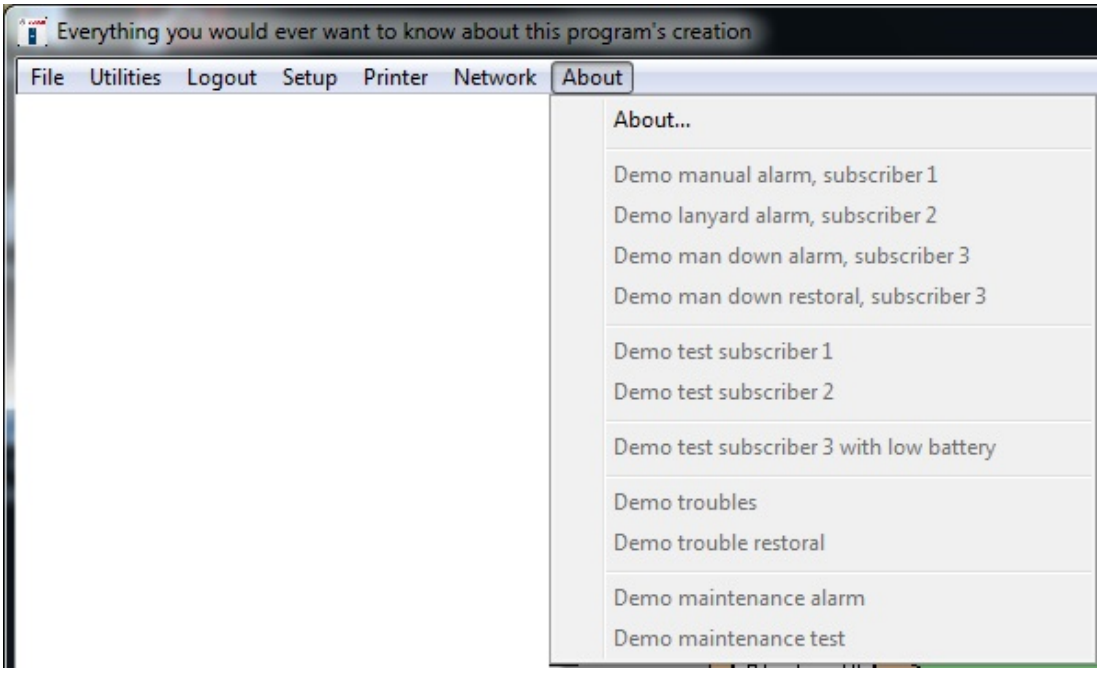


Figure 8.32: About Menu

Demo manual alarm, subscriber 1 For demonstration only, and can't be used in a live system. It causes system to display an alarm from the subscriber with transmitter ID number 1. In the **System Preferences** dialog, select **Enable Demo Selections** checkbox to enable these demo alarm and trouble selections. The transponder communication ports and network communication ports must also be disabled, and the operator of the system must login at "Installer" or "Installer Master" authority level.

Demo lanyard alarm, subscriber 2 For demonstration only, and can't be used in a live system. It causes system to display a lanyard alarm from the subscriber with transmitter ID number 2.

Demo man down alarm, subscriber 3 For demonstration only, and can't be used in a live system. It causes system to display a man down alarm from the subscriber with transmitter ID number 3. The man down alarm is delayed by the programmed man down delay (usually 10 seconds).

Demo man down restoral, subscriber 3 For demonstration only, and can't be used in a live system. It will restore a previous man down alarm from the subscriber with transmitter ID number 2, if it has not timed out and is not being displayed.

Demo test subscriber 1 For demonstration only, and can't be used in a live system. It simulates a test from the subscriber with transmitter ID number 1.

Demo test subscriber 2 For demonstration only, and can't be used in a live system. It simulates a test from the subscriber with transmitter ID number 2.

Demo test subscriber 3 with low battery	For demonstration only, and can't be used in a live system. It simulates a test from the subscriber with transmitter ID number 3. This test also reports low battery.
Demo troubles	For demonstration only, and can't be used in a live system. It simulates troubles from a transponder. Point troubles are simulated for AC loss, tamper and no response. Transponder troubles are simulated for remote key and remote key tamper. The individual troubles can be enabled or disabled in the **Popup Trouble Filter** dialog. The trouble delay in the **Popup Trouble Filter** dialog will also affect these troubles. Therefore, for demo purposes, it should be set to 0.
Demo trouble restoral	For demonstration only, and can't be used in a live system. It simulates trouble restorals for all the troubles sent in **Demo Troubles**.
Demo maintenance alarm	For demonstration only, and can't be used in a live system. It simulates an alarm from a maintenance transmitter.
Demo maintenance test	For demonstration only, and can't be used in a live system. It simulates a test from a maintenance transmitter.

8.6.1 About dialog

The **About** dialog presents the version information, copyright data and internal processing timers.

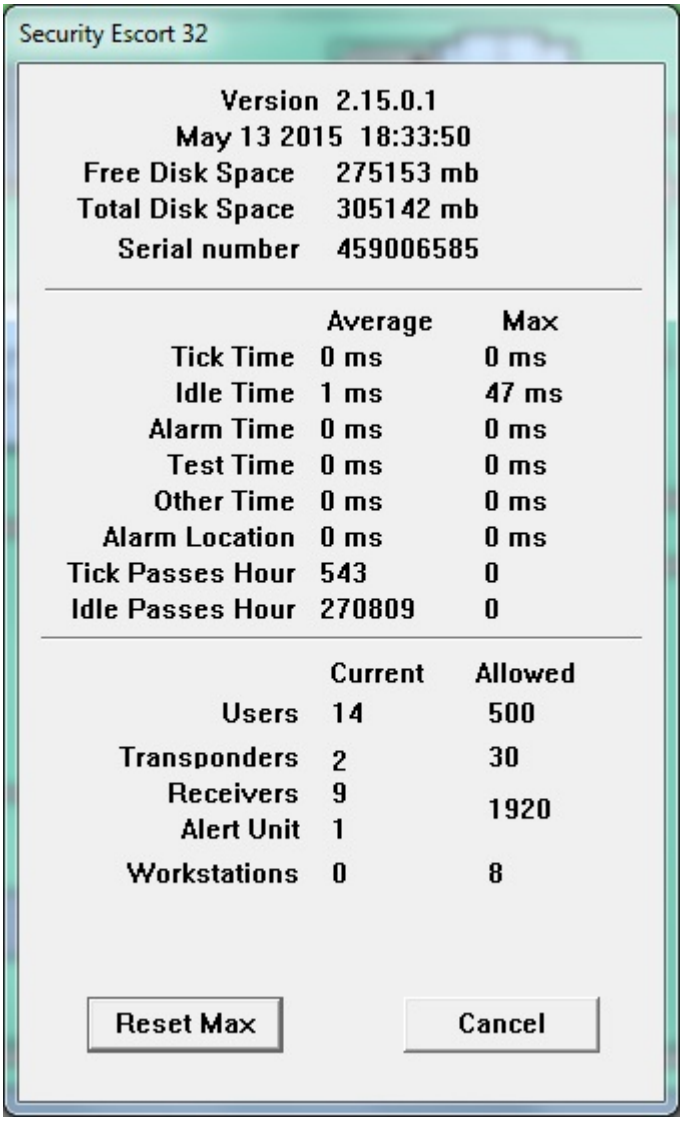


Figure 8.33: About Dialog

Version	At the top of the dialog, the software version and the date and time that it was compiled, is displayed.
Free Disk Space	This shows the free disk space on the “C” drive of this computer.
Total Disk Space	This shows the total disk space on the “C” drive of this computer.
Tick Time	The amount of time spent in the time tick processor per pass.
Idle Time	The amount of time spent In the idle time processor per pass.
Alarm Time	The amount of time spent to process each alarm report from a transponder.

Test Time	The amount of time spent to process each test report from a transponder.
Other Time	The amount of time spent to process each trouble and other message reports from a transponder.
Alarm Location	The amount of time spent to compute an alarm location.
Tick Passes Hour	The number of passes through the tick time processor that occurred in an hour.
Idle Passes Hour	The number of passes through the idle time processor that occurred in an hour.
Serial number	Displays the serial number of this Security Escort System installation as read from the software key.
Maximum users	Displays the maximum number of users that this Security Escort System installation allows. This number is programmed into the software key.
Max transponders	Displays the maximum number of transponders that this Security Escort System installation allows. This number is programmed into the software key.
Max workstations	Displays the maximum number of workstations that this Security Escort System installation allows. This number is programmed into the software key.
[Reset Max]	Resets all of the max timers.

9 Files required for Security Escort

The following files must be in the same directory as ESC32.EXE (default “C:\ESCORT”).

Files	Description
Esc32.exe	the main program
Bwcc32.dll	support for the dialog appearance
Cdrvdl32.dll	communications support
Cdrvhf32.dll	communications support
Cdrvxf32.dll	communications support
Commsc32.dll	communications support
W32mkde.exe	the database manager
W32mkrc.dll	support for the database manager
Wbtrcall.dll	support for the database manager
Wbtrv32.dll	support for the database manager
Lfbmp70n.dll	support for the screen images
Lfcmp70n.dll	support for the screen images
Ltkrn70n.dll	support for the screen images
Ltfil70n.dll	support for the screen images

The following files are the preferences for this workstation and are stored in the same directory as ESC32.EXE.

Files	Description
Wprefers.edb	the workstation preferences settings
Prefersc.edb	Old system preferences settings. This file is converted to gprefers.edb and wprefers.edb, and then is automatically deleted.

The map of the facility is a standard Windows bitmap (BMP) file. It must be stored in the same directory as ESC32.EXE.

Files	Description
MAP0.EDB	Main map bitmap file.
MAP1.EDB	Extra map bitmap file if used.
MAP2.EDB	Extra map bitmap file if used.

The following files are the system databases that are stored at the Master Database path (duplicate copy in the Slave Database Path).

Files	Description
Operator.edb	System Operators Database
Preferen.edb	System Preferences settings
Reports.edb	Alarm Reports database
Subscrib.edb	Database of the Subscribers/ Transmitters
Transpon.edb	Database of the System Configuration
Gprefers.edb	Global system preferences settingss

The following sound files should be in the Windows\media directory:

Files	Description
SEtroubl.wav	trouble sound
SEalarm.wav	alarm sound

These are sample images for demo and test. The following files should be in the IMAGES directory, which is a sub-directory to the ESC32.EXE directory (default “C:\ESCORT\IMAGES”)

Files	Description
Image1.jpg	sample subscriber image
Image2.jpg	sample subscriber image
Image3.jpg	sample subscriber image

Notes

Notes

Notes

10 Appendix: Software licenses

This product contains both software that is proprietary Bosch software licensed under the Bosch standard license terms, and software licensed on the basis of other licenses.

10.1 Bosch software

All Bosch software © Bosch Security Systems. Bosch software is licensed under the terms of the End User License Agreement (EULA) of Bosch Security Systems B.V. or Bosch Security Systems Inc, as available together with the physical carrier (CD or DVD). Any use is subject to agreement and compliance with such EULA, as applicable.

10.2 Other licenses — copyright notices

Bosch is committed to comply with the relevant terms of any open source license included in its products. The open source licenses for Security Escort 2.15 are listed in the **OpenSourceLicensing.doc** file in the Open Source folder of the CD-ROM. The relevant open source software or source code can also be obtained by downloading from the Bosch product catalog website.

10.3 Warranties and disclaimer of warranties

Software provided under other licenses has specific disclaimers of warranties. These are repeated in the full license texts, and apply in full to the relevant software components. All software components provided under the other licenses are provided "as is" without any warranty of any kind, including but not limited to any implied warranty of merchantability or fitness for a particular purpose, unless stated otherwise in writing. Please see the full text of the relevant software licenses for further details. The Bosch standard product warranty only applies to the combination of hardware and software as delivered by Bosch. Without prejudice to any licensee's right to apply the provisions of a relevant software license, any modification of any software delivered with or as part of the product may render any warranty on the whole product or any parts thereof null and void, and Bosch is entitled to charge fees for any services in relation thereto.

Index

Symbols

-, 85
+, 85

A

Abort setup for this MUX point, 200
About dialog, 217
About menu, 215
AC loss, 192, 193
Acknowledge, 145, 146
Acknowledge subscriber type, 129
Add, 142
Address, 130
Advanced, 131
Alarm, 116
    maintenance, 174
Alarm area setup, 90
Alarm Background Color, 130
Alarm differential, 195
Alarm group, 139
Alarm group #, 144
Alarm group name, 144
Alarm Group State dialog, 145
Alarm Groups dialog, 144
Alarm Location, 219
Alarm map, 170
Alarm min level, 195
Alarm on open loop, 138
Alarm on shorted loop, 138
Alarm report
    incomplete, 172
Alarm Reports Database, 168
Alarm spot size, 117
Alarm Time, 218
Alarm type definitions, 124
Alarm voice output, 121
Alarm when armed, trouble when disarmed on open loop, 138
Alarm when armed, Trouble when disarmed on shorted loop, 138
Alarm zone, 118, 130
Alarms, 188
Alert, 86
Alert unit
    estimating number of, 26
Alert units to receivers, 86
Algorithm, 87
All from Transponder Selected, 188
All Pager Confm Not Reqd, 121
Ambient, 198, 199
Analyze alarms, 189

Answer on ring, 73
answering machine, 73
Answering machine override, 73
Ant map, 199
Antenna, 198
Area definition with polygon, 89
Area number, 91
Arm Time, 143
Arming state of this alarm group, 144
Authority levels, 167
Auto Advance, 198
Auto Reset Comm Ports ‘X’ hours, 122
Auto silence alarm in 'X' seconds, 121
Auto synchronize time, 211
Autobackup to the slave database, 212
Automatic by schedule, 144
Automatic redundancy, 173
Automatically send selected troubles, 206
Average, 201

B

Backup, 180
Backup / restore to disk cartridge path, 213
Backup and restore, 180
Backup databases, 178
Bad checksum, 193
Baud, 72
Baud rate, 207
Beginning, 81
bitmap, 132
BMP, 132
Bring to front on alarm, 116
Bring to front on trouble, 116
Browse, 131
Buddy check, 114
Buffer Overflow, 203
Buffer Overflow Count, 205
Build, 130
Bus -, 85
Bus +, 85
Bus fault, 192
Bus micro revision, 196
Byte, 195

C

Cancel, 90, 127, 131
Cancel page if alarm reset, 207
Carrier Det, 70
Cartridge, 213
Cartridge disk drive, 180
Central Console
  Function of, 11
  minimum system requirements, 11
  software overview, 11
  versions, 11
  wiring, 48, 50
Character limit, 206
Check-in Schedule, 140
Choose Destination Location dialog, 62
City, 130
Classic algorithm, 87
Clear, 126
Clear EE, 196
Clear screen, 185
Close dialog, does not stop test, 202
COM, 70, 71
Comm fail to siren out, 195
Comm Mode, 80
Comm Port Index, 80
Comm port overload, 193
Comm. fail reset, 211
Communications
  failure of, 191
Communications failure, 188
Communications failure messages
  disabling, 81
Compatible parts, 10
Computer
  Master, 73
  remote, 73
  Slave, 73
  workstation, 73
Contact information, 123
Control room, 117
Control room output to siren, 116
Control room output to spare, 116
Control room output to strobe, 116
Copy, 81, 89
CR Only, 72
CR/LF, 72
Created, 80
CTS Control, 70
Current Check-in Status dialog, 145

Cut, 89

D

Daily test report, 183
Daily trouble report, 183
Database backup, 178
Database backup and restore, 188
Database errors, 189
Database find level, 122
Database restore, 180
Databases
operator:editing, 166
reports:map, 170
reports:sorting, 171
subscriber:editing, 125
Databases are not shared, 211
Day month format, 114
Day of the Week, 143
Default Master computer, 73
Default Slave computer, 73
Delete, 171
Delete Point, 81
Demo alarms, 207
Demo lanyard alarm, 216
Demo low battery, 217
Demo maintenance alarm, 217
Demo maintenance test, 217
Demo man down alarm, 216
Demo man down restoral, 216
Demo manual alarm, 216
Demo Test, 216
Demo test subscriber, 216
Demo trouble restorals, 217
Demo troubles, 217
Dialing prefix, 73
Direct connect port, 73
Disability, 129
Disable auto reconnect, 211
Disable idle processing, 115
Disable on shorted loop, 137
Disable open loop, 138
Disabled, 74, 129
Disarm Time, 143
Display maintenance alarm, 115
Display unauthorized alarms, 120
Do not resend alarm page, 207
Done, 132, 140

E

Edit Data, 81, 170
Edit operator record, 166
Edit Schedule Times, 141
Edit Schedule Times dialog, 142
EE counters, 196
EE point info, 196
EE point stat, 196
EE point trouble, 196
Emergency answer only, 73
Enable algorithm tweaks, 115
Enable Rec, 201
Enable reed switch, 137
Enable remote key, 195
End of File, 81
End of shift reminder, 122
Equipment estimation
general, 24
Excel test history files, 116
Export, 184
Exporting a Subscriber Database, 146
Exporting a Transponder Database, 155
Exporting the Subscriber Database, 153
Exporting the Transponder Database, 164
Eye Color, 130

F

Fail to test letters, 184
Failed pager attempts, 203
Failed to Check-in Report, 140
Female, 130
File menu, 174
Files required, 220
Filter virtual fence, 120, 139
First, 144
Fixed location and pager text, 138
Fixed location transmitter, 137
Floor, 91
Floor Level, 86, 137
Floppy A, 180
Force map background erase, 114
Free Disk Space, 218

G

Green Led, 198
Guard tour exception report, 183
Guard tour level, 123
Guard tour minutes, 123
Guard tour report, 183

H

Hair Color, 130
Hardware Overrun, 203, 205
Height, 130
High speed buddy check, 114
Highest, 201
History archive file A, 187
History archive file B, 187
History filter dialog, 186
History filter output, 74
History screen, 187
Hits, 201
Horn - Siren, 198

I

ID Receiver, 117
Idle Passes Hour, 219
Idle processing
    disable, 115
Idle Time, 218
Ignore Communications Failure, 81
Ignore Holidays for this Schedule, 141, 142
Image, 132
Image File, 131
Image file path, 213
Importing a Subscriber Database, 146
Importing a Transponder Database, 155
Importing the Subscriber Database, 153
Importing the Transponder Database, 164
Incoming Communication Errors, 203, 214
Incoming Retried Messages, 203, 214
Incomplete alarm report, 172
Indoor receiver installation, 28
Information, 131
Information field labels, 124
Insert New, 81
Insert new transponder, 83
Installation Complete dialog, 65
Installation procedure, 60
Installation starts
    progress, 65
Installer alarms silent, 121
IP Address, 80
Isolate From All Other Transponders For Location, 80

J

Jam map, 199
Jamming, 199
Jamming of receiver, 193
JPG, 132

K

Key Select, 172
Kill Transponder, 81
Known transmitters, 193

L

Lantronix interface
    DB25 pinouts, 51
    wiring, 50
Last, 145
Last MUX message, 196
Last Remote Access Time, 203
Learn address button, 212
LF Only, 72
Limit alarms to 1 transponder, 120
Limit alarms to one area, 120
Linear algorithm, 87
Linear depth, 117
Load delay, 195
Local Escort drive, 180
Local Escort path, 213
Locate, 89, 137
Locate Key, 171
Locate test level, 123
Locate transmitters, 174
Location, 86
    estimate of, 174
    Text to be displayed, 86
Location accuracy, 23, 26, 110, 112
Location algorithm, 87
Login changes, 189
Loop communications, 194
Low battery
    alert unit, 193
    transponder, 192
Low battery report, 183
Low depth, 118
Low pull algorithm, 87
Lowest, 202

M

Maintenance "alarm", 175
Maintenance alarm, 115, 174
Maintenance transmitter, 199
  use in setup mode, 199
Male, 130
Man down Alarm On Auto track, 120
Man down delay timer ‘X’ seconds, 122
Man down jitter timer ‘X’ seconds, 122
Manual redundancy, 173
Map, 87
  alarm, 170
Map file generation, 68
Map file scaling, 68
Map number, 137
Map scale %, 117
Map X position, 137
Map Y position, 137
Master computer, 73
Master computer answers, 73
Master computer switch, 189
Master Database drive, 179
Master Database path, 212
Master’s Network Address, 211
Master's Network Listen Port, 211
Max Low Battery Messages, 204
Max Man Down Messages, 204
Max Receiver Buffer, 205
Max Report Spooler Bytes, 205
Max Spooler Bytes, 204
Max Test Strobe Messages, 204
Max Transmit Buffer, 205
Max transponders, 219
Max workstations, 219
Maximum Alarm Messages, 204
Maximum Retry Messages, 204
Maximum Trouble Messages, 204
Maximum users, 219
Medium depth, 118
Medium pull algorithm, 87
Merging a Subscriber Database, 146
Merging the Subscriber Database, 155
Midnight report, 184
Minimum system requirements, 11
Missed all receivers, 201
Misses, 201
modem, 115
Modem communications, 189
Modem init, 74, 207
Modem Port, 71
Modem reset, 74
Modfying existing transponder, 83
Modified, 80
Modify Oper, 80
Moinitor supervisions, 115
Mon Power, 70
Monitor communications, 115
Monitored periods, 193
Moxa interface
  DB9 pinouts, 48
  wiring, 48
Moxa/Lantronix
  troubleshooting, 103
Multiple map files, 68
Multiplex point
  address, explanation of, 81
Multiplex receiver
  for automatic ID# capture, 117
Multiplex receiver parameters, 83

N

Name, 130
National Electrical Code, 31
Network comm failure, 193
Network communications, 189
Network Port, 71
Network status dialog, 202
New alarm reports, 183
New ID, 130
Next, 81, 145, 195, 197
No buddy check delay, 115
No CTS, 70
No password on reentry, 116
No password timeout, 116
No password to exit, 116
No point text if area text, 120
No receiver icons, 121
No response
  from multiplex device, 193
No Restriction, 188
Not always top window, 116
Not testing report, 183

O

Off, 198
Off (disarmed), 144
On, 198
On (armed), 144
On outside tests, flash strobe for 'X' seconds, 122
Only From Transponder Selected, 188
Open loop alarm, 138
Open loop disable, 138
Open loop trouble, 138
Operator activity log, 188
Operator Database, 166
Operator database changes, 188
Optional parameter, 194
Optional text, 137
Other Time, 219
Outdoor receiver installation, 28
Outgoing Retried Messages, 203, 214
Output device error, 193
Output includes subscriber ID, 120
Output includes transmitter ID, 120
Output verification, 185
Overload Count, 205
Overload Level, 205

P

Page to individuals, 208
Pager
  send message, 207
Pager communications, 115
Pager confirmation not required, 137
Pager Group, 91, 207, 208
Pager groups, 137
Pager ID, 137, 206
Pager password, 136
Pager setup, 205
Pager text Manual, 208
Pages per call, 206
paging service, 206
Password, 74, 116, 166, 206
Password verify, 74
Paste, 89
Personal Ttransmitter
  automatic capture of ID#, 117
Pervious, 144
Phone, 130
Phone number, 136, 206
Point, 117, 201
Point troubles, 189
Point Type, 85, 86, 87
Points, reporting alarm, 188
Polygon to define area, 89
Pop-up trouble and pager delay, 194
Popup trouble filter dialog, 190
Port No., 80
Power loss
  alert unit, 193
  transponder, 192
Pre-construction coverage verification survey, 26
Preferences changes, 188
Previous, 81, 195, 196
Print, 81, 126, 127, 184
Print file dialog, 208
Print Report, 145, 146
Print report now, 184
Print Subscriber Database, 126
Print System Reports dialog, 184
Print/Export System Reports dialog, 182
Printer, 187
Printer output, 189
ProxLink
  configuration, 56
  setup, 56
  troubleshooting, 101

Pulse dial, 73
Put this receiver in setup mode, 198, 199

R

Radio ID, 80
RAM counters, 196
RAM EE buss fault, 196
RAM EE mstat batt, 196
RAM point info, 196
RAM point stat, 196
RAM point trouble, 196
Readme Information dialog, 61
Recall operator in 'X' seconds, 122
Receive Level Maps, 189
Received signal strength
  checkbox for displaying, 115
  measuring with maintenance transmitter, 174
Receiver
  configuration, 108, 197
  determining receiver location, 26
  installation, 28
  system power up, 93, 108
  testing receiver spacing, 26
  troubleshooting, 105
Receiver 1, 87
Receiver 2, 87
Receiver Buffer Max, 203, 214
Receiver configuration dialog, 197
Receiver parameters, 83
Receiver sensitivity adjust, 88
Receiver test dialog, 200
Receivers
  estimating number of, 24
Receivers not heard from report, 183
Red Led - Strobe, 198
Reed switch, 137
Refresh Data, 203, 205, 215
Remote comm port setup dialog, 70
Remote computer, 73
Remote Control Listening Port, 212
Remote key activation, 192
Remote key tamper, 192
Remote setup dialog, 72
Remote system control, 74
Remove >>, 142
Report
  End of shift reminder for, 122
  trouble, filtering, 190
Report database changes, 188
Reports Database, 168
Require alarm report, 121
Requires check-in, 140

Requires restore, 139
Reset, 126
Reset Max, 219
Reset point, 199
Reset Status, 203, 205, 215
Reset to Default, 195
Restore database, 180
Restore to disk cartridge path, 213
Revision, 199
RF micro revision, 198
RF point troubles, 188
Run buddy check, 114
Run silent, 194
Run test, 202

S

SA%, 88
Save, 90, 131
Save EE, 196
Scaling, 213
Schedules dialog, 140
SE485 interface adapter
troubleshooting, 100
Security alarms silent, 121
Security pager, 207
Security Pager Confm Not Reqd, 207
Security preferences, 118
Security Preferences dialog, 139
Select Point dialog, 84
Send all other alarms, 207
Send change, 195
Send installer demo alarms, 207
Send page a second time, 2 minute delay, 207
Send pager message dialog, 207
Send Security, 208
Send Service, 208
Send to group, 208
Sensitivity adjust, 88
Serial number, 219
service pager, 206
Setup Type dialog, 64
Shift reminder, 122
Shorted loop alarm, 138
Shorted loop disable, 137
Shorted loop trouble, 138
Show all error pop-ups, 211
Show Areas, 83
Show connection pop-ups, 211
Show History, 186
Show maintenance levels, 115
Show Map, 186
Show personal data, 121
Show Points, 83
Show test levels, 115
Show tests on the map, 121
Silent, 129
Site survey, 26
General, 23
Slave computer, 73
Slave computer answers, 73
Slave Database drive, 180
Slave Database path, 213
Slave's Network Address, 211
Slave's Network Listen Port, 211

Sound maintenance alarm, 115
Sound unauthorized alarms, 120
Spacing, 202
Spare, 195
Spare 2, 188
State, 130
Stop all pages, 208
Stop test and reset counters, 202
Strong depth, 118
Strong pull algorithm, 87
Subscriber
  advanced features dialog, 135
Subscriber Check-in report, 184
Subscriber class names, 123
Subscriber Database, 125, 135, 146, 153, 155
Subscriber database changes, 188
Subscriber Database editing, 127
Subscriber ID, 130
Subscriber image Extension, 213
Subscriber image file path, 213
Subscriber image Scaling, 213
Subscriber images, 132
Subscriber Type, 129
Successful Incoming Messages, 203, 214
Successful pager messages, 203
Sunday report, 184
Supervise unauthorized, 114
Supervision Duration, 130
Supervision Location report, 184
Supervision monitor, 188
Supervision Monitors, 204
Supervision period, 139
Suppress Lanyard Alarm, 121
Suppress Man Down Alarm, 121
Synchronize system time, 185
System block diagram, 9
System Defaults dialog, 123
System Labels dialog, 124
System name, 207
System phone, 207
System power up, 91
System preferences
  setting, 113
System preferences dialog, 113
System redundancy, 172
  automatic, 173
  manual, 173
System Serial, 71
System serial port, 187
System status dialog, 204

T

Tamper, 193
  transponder, 192
Tamper load, 195
Test, 86, 115
Test differential, 195
Test min level, 195
Test on this MUX point SUCCESSFUL, 200
Test receiver, 195
Test Time, 219
Test transmitter type, 195
Tests including point Info, 188
Tests, single line, 188
This schedule defines the check-in times, 141
Tick Passes Hour, 219
Tick Time, 218
Titles for subscribers, 124
tone dialing, 73
Total Disk Space, 218
Total Outgoing Messages, 203, 214
Total Remote Access Connections, 203
Total transmissions, 201
Total Wrong Access Code Attempts, 203
Transmit, 199
Transmit Buffer Max, 203, 214
Transmit delay, 195
Transmit point, 195
Transmitter
  exchanging, 175
  location, 174
Transmitter Change, 175
Transmitter ID, 130
Transmitter low battery, 188
Transmitter supervision duration, 130
Transmitter Type, 129
Transmitting Point, 201
Transponder, 195, 201
  database, 79
  Database:creating new entry, 82
  estimating number of, 26
  removing from database, 81
  system power up, 92, 93, 108
  troubleshooting, 100, 101, 103, 104
Transponder area, 139
Transponder comm port setup dialog, 70
Transponder communication, 188
Transponder data changes, 188
Transponder data view, 189
Transponder data view dialog, 195

Transponder Database, 155, 164
Transponder Database dialog, 79
Transponder ID, 80
Transponder maps, 189
Transponder name, 79, 138
Transponder parameter change dialog, 194
Transponder point number, 84
Transponder restriction, 188
Transponder startup, 192
Transponder troubles, 189
Transponder Type, 79
Trigger all the outputs on alarm 'X' seconds, 122
Trouble, 116
    Emergency contact text box for, 123
Trouble on open loop, 138
Trouble on shorted loop, 138
Trouble Response Text, 83
Trouble Tamper Text, 83
Trouble Type Text, 83
Troubles, 206
Turn on alarm strobes, 119
Turn on outside sounders, 119

U

Unknown transmitters, 193
Uses Proxim radio, 195
Utilities menu, 178

V

Verbose point reports, 195
Version, 218
Video Switcher, 91
Video switcher control, 74
Video switcher restore, 74
View Alarm Groups, 141
View Alarm Groups dialog, 143
virtual fence, 89, 120
Virtual fence alarm, 91, 138, 139
Virtual Fence Area, 91
Virtual receiver, 87
Virtual receiver Point Type, 87

W

Wandering alarm, 91
Wandering alarms, 89
Watchdog minutes, 123
Weekly maintenance test report, 184
Weekly security test report, 184
Weekly subscriber test report, 184
Weekly watchman test report, 184
Wiring
    general, 30
    Lantronix, 50
    Moxa, 48
    SE485, 30
Wondering alarm, 139
Workstation computer, 73
Write EXCEL import file, 127

Z

Zip, 130

Robert Bosch (SEA) Pte Ltd
11 Bishan Street 21
573943 Singapore
Singapore
www.boschsecurity.com
© Robert Bosch (SEA) Pte Ltd, 2015

Bosch Sicherheitssysteme GmbH
Robert-Bosch-Ring 5
85630 Grasbrunn
Germany